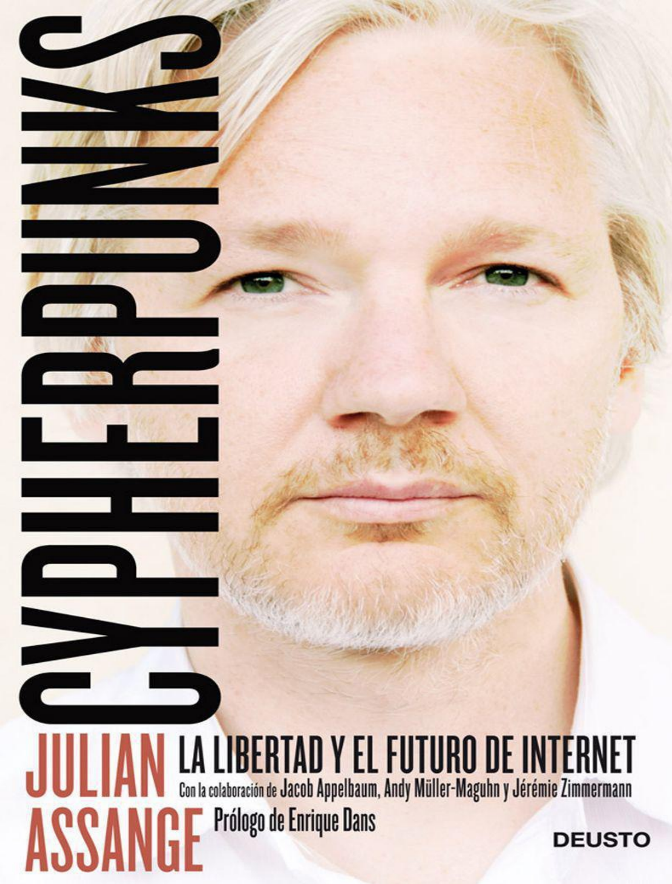


CYPHERPUNKS

JULIAN ASSANGE

LA LIBERTAD Y EL FUTURO DE INTERNET

Con la colaboración de Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann

Prólogo de Enrique Dans

DEUSTO

Índice

Prólogo

Para cualquier persona a quien la red genere algún tipo de impresión positiva, para cualquiera que vea en internet un lugar para acceder a información, para comunicarse o para tantas otras cosas que hacemos habitualmente en nuestro día a día, este libro será, sin lugar a dudas, una lectura amarga. No, no espere que su lectura le resulte en absoluto agradable. Ni por el formato escogido, que no resulta el más fácil de consumir, ni por su contenido, que se despliega lentamente ante los ojos del lector, frase a frase, a medida que la conversación va tocando más y más temas, hasta construir un escenario verdaderamente desasosegante.

No, el libro que tienes entre las manos no es un libro agradable. Está repleto de malas noticias, de augurios pesimistas y de llamadas de alerta. Noticias, augurios y alertas, además, hechos «desde el otro lado», por personas que han tenido la oportunidad de mirar directamente a los

ojos del enemigo, de sufrir su persecución. Un enemigo invisible, de magnitud descomunal, que pretende controlar todos nuestros pasos, todas nuestras acciones, todos nuestros pensamientos. Un enemigo al que no siempre vemos, que acecha nuestras conexiones, que recopila nuestra información, que investiga por dónde navegamos, con quiénes nos conectamos y qué les decimos, que pretende saber más de nosotros que nosotros mismos. Un enemigo dispuesto a lo que sea por mantener un delicado equilibrio en el que se sabe ganador: en situación de asimetría informativa, siempre termina ganando el que todo lo ve.

El autor principal que firma este libro lleva desde junio de 2012 encerrado en una embajada, sin poder poner un pie en la calle, sometido a un acoso absolutamente impropio. Se ha visto perseguido, acusado de delitos con una base absolutamente absurda, y amenazado de muerte por políticos de países supuestamente civilizados. Ha podido comprobar lo que pasa cuando tu organización es perseguida hasta el punto de cortarle todas sus posibles fuentes de financiación, lo que ocurre cuando, en una absoluta falta de respeto a las leyes y a las relaciones internacionales, se presiona a quienes deberían ser medios de pago neutrales para convertirlos en supuestos guardianes morales del dinero de sus usuarios. Utilizando VISA, Mastercard o PayPal puedes hacer donaciones al Ku

Klux Klan, a organizaciones pronazis o a entidades que defienden el odio o el uso de la violencia... pero no puedes contribuir a financiar a Wikileaks. Si lo intentaste en su momento, tienes muchas posibilidades de que tu dinero, simplemente, no llegase a tu destino. Si lo intentas ahora, tendrás que buscar métodos alternativos, porque lo normal es que te encuentres con que, sencillamente, no es posible. Si, en un arrebato de moralidad, decides prescindir de los servicios de esas empresas que te impiden hacer lo que quieres con tu dinero y donar a una causa que estimas justa, te encontrarás con que es extremadamente difícil, en el mundo en que vivimos, hacer una vida mínimamente normal sin ellas

Wikileaks es el signo de los tiempos: el desarrollo y popularización de la red como herramienta en manos de una parte significativamente mayoritaria de las sociedades desarrolladas ha determinado que muchas de las cosas que antes tenían lugar en secreto, dejen de transcurrir en la oscuridad. La red es la herramienta más poderosa para que los ciudadanos en las sociedades democráticas pongan en práctica una supervisión completa sobre las actividades de sus teóricos representantes, los políticos. Pero ante una herramienta así, surge un problema de primera magnitud, una disfuncionalidad manifiesta: hacía ya mucho tiempo que esos teóricos representantes de los ciudadanos habían dejado de representarlos, para pasar a representarse a sí

mismos y a sus intereses particulares. Con algunas honrosas pero escasas excepciones, la primera preocupación de un político en nuestros días es la llegada a su cargo y la preservación del mismo, seguida por la consecución de fuentes de ingresos en el hipotético caso de que tenga que abandonar el mismo. Así, los políticos se convierten en gestores de favores a cambio de un enriquecimiento más o menos obvio, que alimenta desde la corrupción directa hasta el tratamiento privilegiado a determinados lobbies en función de intereses que, en muchos casos, no coinciden en absoluto con los de los ciudadanos que, con sus votos, situaron a ese teórico representante público donde está.

Pocas cosas están más justificadas en la vida pública que la transparencia. Por el hecho de serlo, un político, por su condición de representante y servidor de los ciudadanos, debería tener un deber de transparencia absoluto: deberíamos saber qué hace, dónde está en cada momento, con quién o quiénes se reúne, de qué temas habla, qué acuerdos o promesas compromete, su agenda, sus opiniones en todos los temas relevantes... desempeñar la función pública debería exigir una garantía de transparencia total en todo, incluidos por supuesto los ingresos y los gastos.

En un mundo así, con políticos y gobiernos comprometidos con ese nivel de transparencia, Wikileaks no sería en absoluto necesaria. Hoy, la tecnología proporciona todas las herramientas necesarias para que esa transparencia

tenga lugar. Podemos saber en todo momento dónde está una persona, y podemos además proporcionarle herramientas para que informe de todos sus pensamientos, reuniones o decisiones. Pero en su lugar, lo que los políticos y los gobiernos están haciendo es pretender utilizar la tecnología no para que los ciudadanos les exijan esa transparencia, sino para imponer a esos mismos ciudadanos una vigilancia que en modo alguno esos ciudadanos desean ni estiman conveniente. En lugar de utilizar la tecnología para controlar al poder político, el poder político pretende utilizar la tecnología para controlar a los ciudadanos. Un giro completamente inaceptable, contra el que WikiLeaks pretende luchar.

WikiLeaks es un gestor de información. En su funcionamiento, WikiLeaks intenta reducir en la medida de lo posible las barreras de entrada al llamado *whistleblowing*, al filtrado de información. Cuando una persona maneja información que, por la razón que sea, estima debería ser pública, WikiLeaks procura ofrecerle modos libres de riesgo para, de manera efectiva y eficiente, hacerla pública. Mediante esquemas de anonimato, protección de las fuentes, verificación de la información, estudio de las consecuencias legales, y difusión viral, WikiLeaks procura asumir una función que, en muchos casos, la prensa tradicional ya no es capaz de ejercer. Los vínculos de la prensa tradicional con el poder, los esquemas de

financiación mediante publicidad institucional, la escasa diligencia en la protección de las fuentes o la nula voluntad de asumir determinados riesgos han provocado que el hecho de «tirar de la manta» en un tema llevándolo a la prensa implique una ruta como mínimo compleja, llena de incertidumbres y peligros que muy pocos podrían asumir. WikiLeaks, en ese sentido, es toda una llamada de atención al periodismo: no trabaja al margen del mismo, utiliza sus esquemas par dar salida a la información, pero diseña, apoyándose en la red, toda una nueva esquemática de trabajo que permite a quien lo estime oportuno convertirse en fuente. Y el esquema, como prueban las muchísimas revelaciones que ha logrado sacar a la luz, funciona.

Por mucho que pueda parecer a mentes clásicas, conservadoras o supuestamente biempensantes, el mundo está mucho mejor con WikiLeaks. Por provocativo y peligroso que suene el que la información se intercambie a la vista de todos o el que la política se celebre en espacios abiertos, el clima de secretismo en que se desarrollaba la gestión de los gobiernos no sólo no estaba diseñado para servir a los ciudadanos, sino que cada día existían más evidencias de todo lo contrario, de que estaba creado para servir a los intereses de terceros, a intereses en absoluto legítimos. La transparencia en la gestión pública sólo debería responder a dos limitaciones: la intimidad de los ciudadanos y las leyes de secretos oficiales, que deberían regularse con

absoluto rigor para que fuesen utilizados únicamente en las ocasiones en las que fuese estrictamente necesario. Todo lo demás, en un mundo hiperconectado, debería sencillamente eliminarse.

En su lugar, los gobiernos están utilizando la red para dar lugar al mayor aparato de espionaje y vigilancia de los ciudadanos que ha existido nunca. Estamos viviendo una realidad que convierte a George Orwell en el más grande de los visionarios, una dinámica con muy pocas posibilidades de vivir una marcha atrás. La libertad de la que disfrutamos en internet desde su creación y popularización se nos está escapando entre los dedos, está desapareciendo a toda velocidad, mientras todo un conjunto de tecnologías como las cámaras, los sistemas de reconocimiento facial, la cibervigilancia, la *deep packet inspection*,[1] los filtros o la retención de datos van convirtiendo el mundo en que vivimos en un entorno completamente diferente, en una dura realidad que nos va a costar mucho trabajo explicar a nuestros descendientes. Cabalgando junto a jinetes del Apocalipsis como la protección de los derechos de autor, la pornografía infantil o la amenaza terrorista nos están trayendo recortes de derechos y libertades sin precedentes, supuestamente en aras de un bien común, desdiciendo a aquel Benjamin Franklin que con tan buen juicio aseveraba que «aquellos que sacrifican libertad por seguridad no merecen tener ninguna de las dos».

Los recortes que comenzaron en regímenes totalitarios, dictatoriales o teocráticos en los que parecía completamente lógico que surgiesen como medio de preservar el statu quo se han trasladado a democracias teóricamente consolidadas sin ningún tipo de solución de continuidad. Que Ahmadinejad en Irán, Ben Ali en Túnez o Mubarak en Egipto reaccionasen al uso de la red para movimientos insurgentes intentando bloquearla y tratando de establecer sobre ella un sistema de vigilancia de la población parecía lógico y hasta esperable: que ese movimiento tenga lugar en los Estados Unidos o en muchos otros países con tradición democrática debería resultar completamente inaceptable, una auténtica causa de revolución. Pero esa, y no otra, es la realidad que estamos viviendo. La realidad sobre la que este libro pretende alertarnos.

El ciberespacio, en todos los sentidos, se ha militarizado. El equivalente de lo que está ocurriendo en la red situado en la calle, fuera de la red, sería directamente la ley marcial. La red y el libre intercambio de información podrían estar posibilitando un período histórico que supusiese el mayor y más vibrante progreso a todos los niveles, pero están en su lugar alumbrando la época más oscura, autocrática y totalitaria que el ser humano ha vivido jamás. Internet, lo creamos o no, se está convirtiendo en el enemigo, en la sustancia que engrasa una pendiente peligrosísima que la humanidad recorre a toda velocidad, en

el mayor y más efectivo facilitador del totalitarismo. Como el propio Assange dice en su introducción, y por mucho que nos pueda costar entenderlo a los que amamos la red como herramienta de libertad, internet en su expresión actual, se ha convertido en una amenaza para la civilización humana.

No existe una forma de escapar a este sistema. Sí, al menos, de luchar contra él, de intentar convertirse en un obstáculo a esa deriva. Y es precisamente lo que Julian Assange y sus compañeros de charla llevan haciendo desde hace ya bastantes años: intentar entender el funcionamiento del sistema todo lo posible y desarrollar al límite la criptografía para tratar de oponerse al mismo. Por esa razón, para entender su importancia y para colaborar con ello, debes comprar y leer este libro. Comprarlo, porque con ello conseguirás que una parte del precio del libro llegue a Julian Assange y a WikiLeaks. Leerlo, porque por duro, espeso y oscuro que te pueda parecer, te estará preparando para entender una realidad que, por estar escondida en complejos e inabarcables esquemas internacionales, es muy posible que no te hayas llegado todavía a plantear.

Tomada en conjunto, lo que tenemos encima es una auténtica cruzada liberticida, lo viejo atacando a lo nuevo, con unas proporciones que resultan casi imposible de imaginar. Nada, ni la propiedad intelectual, ni la lucha antiterrorista, ni la protección de los menores, ni el derecho al honor, ni los derechos de los creadores, ni nada de nada,

por execrable que parezca, justifica la barbaridad que estamos viviendo ni los excesos liberticidas que se nos están viniendo encima. Sólo son, por terribles que parezcan, meras excusas, medios para conseguir un fin.

¿Es imparable? ¿Habían ganado incluso antes de empezar? ¿Son ellos una generación perdida de nostálgicos reaccionarios del pasado cuyas tumbas acabaremos pisoteando con inmenso alivio para asegurarnos de que están bien muertos? ¿O somos nosotros un grupo de ilusos que creyeron durante unos pocos años, que la libertad era posible, y que terminaron convirtiéndose en un simple oasis momentáneo de esperanza, en una simple panda de románticos subversivos trasnochados, de *cypherpunks*?

El ciberactivismo es la única salida que nos queda.

ENRIQUE DANS,
autor de *Nada va a cambiar* (Deusto, 2010)

¿Qué es un *criptopunk*?

Los criptopunks defienden el uso de la criptografía y otros métodos afines como medios para conseguir el cambio social y político.[1] El movimiento, fundado en el año 1990, ha sido especialmente activo durante las *guerras criptográficas* de la década de los noventa y tras la primavera virtual de 2011. El término criptopunk proviene de la unión las palabras *Cypher* (clave, cifra, código criptográfico) y *punk*, y se incorporó al Oxford English Dictionary en el año 2006.[2]

Introducción

Este libro no es un manifiesto. No hay tiempo para eso. Este libro es una advertencia.

El mundo no se desliza sino que galopa sin tregua hacia una nueva *distopía* transnacional. Esta evolución no se ha reconocido adecuadamente fuera de los círculos de seguridad nacionales. Se oculta tras el secretismo, la complejidad y la magnitud que esta evolución comporta. Internet, nuestra mayor herramienta de emancipación, se ha transformado en la facilitadora más peligrosa del totalitarismo jamás vista. Internet es una amenaza para la civilización humana.

Estas transformaciones se han sucedido en silencio porque aquellos que saben lo que está pasando trabajan en la industria de la seguridad global y carecen de incentivos para contarlo. Si dejamos que las cosas discurran naturalmente, en unos pocos años la civilización global se

convertirá en una distopía posmoderna de vigilancia de la que sólo los individuos más capacitados podrán escapar. De hecho, puede que ya hayamos llegado ahí.

Pese a que muchos escritores han valorado lo que internet significa para la civilización global, están equivocados. Se equivocan porque carecen del sentido de la perspectiva que ofrece la experiencia directa. Se equivocan porque nunca han conocido al enemigo.

Ninguna descripción del mundo sobrevive al primer contacto con el enemigo.

Nosotros hemos conocido al enemigo.

Durante los últimos seis años WikiLeaks ha entrado en conflicto con prácticamente todos los Estados de poder y sus respectivos contratistas. Nosotros conocemos el nuevo Estado de vigilancia desde la perspectiva de un infiltrado, porque hemos sondeado sus secretos. Lo conocemos desde la perspectiva del combatiente, porque hemos tenido que proteger de dicho Estado a nuestra gente, nuestras finanzas y nuestras fuentes. Lo sabemos desde una perspectiva global, porque tenemos personas, activos e información en casi todos los países del mundo. Lo sabemos desde la perspectiva del tiempo, porque llevamos años combatiendo este fenómeno y lo hemos visto duplicarse y multiplicarse, una y otra vez. Es un parásito invasivo que se nutre de las sociedades que confluyen en la red. Se expande por todo el planeta infectando a cuantos Estados y personas encuentra

en su camino.

¿Qué debemos hacer?

Érase una vez, en un lugar indeterminado que no era éste ni aquél, ni aquí ni allá, nosotros, un grupo de personas, los constructores y ciudadanos de la joven internet, que debatíamos el futuro de nuestro nuevo mundo.

Observamos que las relaciones entre las personas estarían mediatizadas por nuestro nuevo mundo a medida que fueran fusionándose con él, y que la naturaleza de los Estados, definidos por cómo las personas intercambian información, valor económico y poder, también cambiaría.

Vimos que la fusión entre internet y las estructuras de Estado existentes abría una puerta al cambio de la naturaleza misma de los Estados.

En primer lugar, no hay que olvidar que los Estados son sistemas a través de los cuales fluye la fuerza coercitiva. En el seno de un mismo Estado pueden existir distintas facciones que se disputen apoyos en pro de un fenómeno superficialmente democrático; sin embargo, las bases de los Estados son la aplicación y la evitación sistemática de la violencia. La propiedad de tierras, bienes, rentas, dividendos, los impuestos, las sanciones judiciales, la censura, los derechos de autor y las marcas comerciales, todos están sometidos a la amenazante aplicación de la violencia por parte de los Estados.

La mayoría de las veces ni siquiera nos damos cuenta

de lo cerca que estamos de la violencia, porque todos hacemos cientos de concesiones para evitarla. Como marineros pendientes del viento, rara vez nos damos cuenta de que la superficie terrestre se sustenta sobre múltiples capas de oscuridad.

En el nuevo espacio de internet, ¿qué haría las veces de mediador de esta fuerza coercitiva?

¿Tiene sentido siquiera el hecho de plantear esta pregunta? En este espacio etéreo, en este reino aparentemente platónico de ideas y flujo de información, ¿cabe la noción de fuerza coercitiva? ¿Una fuerza que pudiera modificar documentos históricos, destruir relaciones, interrogar, transformar la complejidad en puro escombro, levantar muros, como un ejército de ocupación? ¿Era un concepto como ése necesario para la cohesión?

La naturaleza platónica de internet, el flujo de ideas e información, está degradada por sus orígenes físicos. Sus cimientos son líneas de cable de fibra óptica que se extienden a través de los suelos oceánicos, satélites que giran sobre nuestras cabezas, servidores alojados en edificios de ciudades que van desde Nueva York a Nairobi y los flujos bancarios que sustentan la economía. Al igual que el soldado que asesinó a Arquímedes mientras éste trabajaba, también podría una milicia armada tomar el control de nuestro reino platónico.

El nuevo mundo de internet, abstraído del viejo mundo

de rudos átomos, no ha alcanzado la independencia. Los Estados y sus amigos asumieron el control de nuestro nuevo mundo al controlar sus puntales físicos. El Estado, como un ejército que cerca un pozo petrolífero, o un agente de aduanas que se deja sobornar, pronto aprendería a aprovechar el control físico que ejercía sobre el valioso espacio para introducirse en el reino platónico. Evitaría así la independencia que habíamos soñado, y luego, ocupando las líneas de fibra óptica y las estaciones terrestres de comunicaciones por satélite, continuaría interceptando masivamente el flujo de información de nuestro nuevo mundo, y toda relación humana, económica y política pasaría a formar parte de una única e intricada red de redes mundial. El Estado infestaría los corazones y el sistema nervioso de nuestras nuevas sociedades, engullendo toda relación manifestada o comunicada, cada página web leída, cada correo electrónico enviado y cada pensamiento *googleado*, y luego almacenaría esta información, un poder insospechado, miles de millones de intercepciones al día, en enormes almacenes ultra secretos. Continuaría explotando este tesoro, el rendimiento intelectual privado de la colectividad humana, con algoritmos de búsqueda y patrones de reconocimiento cada vez más sofisticados, enriqueciendo el tesoro y maximizando el desequilibrio de poder entre el interceptor y el interceptado. Y después aplicaría lo aprendido al mundo físico, para diseñar *drones*

teledirigidos, comités de Naciones Unidas y acuerdos comerciales, y también para favorecer su vasta red de industrias, de infiltrados y amiguetes.

Pero nosotros descubrimos algo. La única esperanza frente a la dominación total, que, con coraje, reflexión y solidaridad podíamos utilizar para resistir. Una extraña propiedad del universo físico que habitamos.

El universo cree en la criptografía.

Es más fácil *encriptar*, es decir, cifrar información, que *desencriptarla* o descifrarla.

Y observamos que podíamos utilizar esta extraña propiedad para crear las leyes de un nuevo mundo. Para sustraer nuestro nuevo reino platónico de las estructuras físicas de satélites y cables submarinos, así como de sus controladores e interceptores. Para fortificar nuestro espacio con un velo criptográfico. Para crear nuevos territorios vetados a aquellos que controlan la realidad física, pues seguirnos en su interior requiere de infinitos recursos.

Y de este modo declarar la independencia.

Así como los científicos del proyecto Manhattan descubrieron que el universo permitía la construcción de una bomba nuclear. Esta conclusión no era evidente antes de plantearse. Tal vez las armas nucleares no formaban parte de las leyes de la física. Sin embargo, el universo sonrió ante las bombas atómicas y los reactores nucleares. Son un fenómeno que el universo bendice, como la sal, el acero o

los rayos X.

Igualmente, el universo, nuestro universo físico, tiene la propiedad de hacer posible que un individuo o un grupo de individuos de manera fidedigna, automática o incluso inconscientemente, codifiquen algo, de modo que todos los recursos y toda la voluntad política de la mayor superpotencia de la tierra no puedan descifrarlo. Y estos senderos de codificación entre personas pueden entrelazarse para crear regiones libres de la fuerza coercitiva del Estado exterior.

De este modo, las personas pueden oponer su voluntad ante la de una superpotencia completamente movilizada y vencer.

La encriptación es la encarnación de las leyes de la física, y no atiende a las bravuconerías de los Estados, ni siquiera a las distopías transnacionales de vigilancia.

No era evidente que el mundo tuviera que funcionar de esta manera. Sin embargo, en cierto sentido, el universo sonríe a la encriptación.

La criptografía es la última forma de acción directa no violenta.

Aun cuando los Estados con armamento nuclear pueden ejercer una violencia ilimitada sobre millones de individuos, la criptografía significa que un Estado, incluso ejerciendo una violencia ilimitada, no puede violar la intención de los individuos de mantener sus secretos fuera

del control de éstos.

La buena criptografía puede resistir la aplicación ilimitada de la violencia. No existe fuerza coercitiva alguna que pueda resolver un problema matemático.

Pero ¿podríamos extrapolar esta peculiaridad del mundo y, de alguna manera, instituirla como bastión emancipador de la independencia de la humanidad en el reino platónico de internet? Y a medida que las sociedades se fusionaran con internet, ¿podría esa libertad reflejarse en la realidad física y redefinir los Estados?

No debemos olvidar que los Estados son los sistemas que determinan dónde y cómo se aplica la fuerza coercitiva de un modo sistemático.

A la cuestión de cuánta fuerza coercitiva puede filtrarse en el reino platónico de internet desde el mundo físico dan respuesta la criptografía y los ideales del movimiento criptopunk.

A medida que los Estados se vayan fusionando con internet y el futuro de nuestra civilización se convierta en el futuro de internet, deberemos redefinir nuestras relaciones de poder con el fin evitar que la humanidad devenga una inmensa red de vigilancia y control masivos.

Debemos dar la voz de alarma. Este libro es el grito del centinela en la noche. El 20 de marzo de 2012, mientras permanecía en arresto domiciliario en el Reino Unido a la espera de la extradición, quedé con tres amigos y

compañeros de vigilancia con la idea de que tal vez alzando nuestras voces al unísono pudiéramos despertar a la ciudadanía. Mientras podamos, debemos contar lo que hemos aprendido.

Nuestra tarea seguirá siendo la de garantizar la autodeterminación allá donde nos sea posible, y contener el avance inminente de la distopía allá donde no lo sea. Y si todo lo demás fracasa, acelerar su autodestrucción.

JULIAN ASSANGE, Londres, octubre de 2012

Participantes en el debate

Julian Assange es el editor jefe y fundador de WikiLeaks.[1] Uno de los primeros colaboradores de la lista de correo Criptopunk, Julian es ahora uno de los máximos exponentes de la filosofía criptopunk en el mundo. Su trabajo con WikiLeaks ha dado una dimensión política a la tradicional yuxtaposición criptopunk: «Privacidad para el débil, transparencia para el poderoso». Si bien su trabajo más visible implica el ávido ejercicio de la libertad de expresión para forzar la transparencia y la responsabilidad de las instituciones poderosas, también es un crítico acérrimo de la intrusión estatal y empresarial en la privacidad de los individuos. Julian es también autor de numerosos proyectos de software acordes con la filosofía criptopunk, como Strobe, el primer escáner de puertos TCP/IP, el programa de encriptación Rubberhorse, y el código original para WikiLeaks.[2] En su adolescencia Julian era un avezado

programador e investigador de la seguridad en la red, antes de que algunos tipos de piratería informática se consideraran legalmente un delito. Convertido a la sazón en activista y proveedor de servicios de red en Australia durante la década de los noventa, Julian también escribió junto a Sulette Dreyfus una historia del movimiento *hacker* internacional, titulada *Underground*, que sirvió de base a la película *Underground: La historia de Julian Assange*.[3]

Jacob Appelbaum es el fundador de Noisebridge en San Francisco, miembro del Club berlinés del Caos Informático y desarrollador.[4] Jacob es uno de los principales defensores e investigadores del Proyecto Tor, un sistema de anonimato virtual creado para que todo el mundo pueda evitar la vigilancia y sortear la censura de internet.[5] Durante la última década se ha centrado en ayudar a activistas medioambientales y pro derechos humanos. Con este mismo fin ha publicado numerosos e innovadores estudios sobre la seguridad, la privacidad y el anonimato en áreas tan dispares como la informática forense o el uso terapéutico de la marihuana. Jacob está convencido de que todos, sin excepción, tenemos el derecho a leer y a expresarnos libremente, sin ningún tipo de restricción. En el año 2010, cuando a Julian Assange se le prohibió dar una charla en Nueva York, Jacob la impartió en su lugar. Desde entonces él, sus amigos y su familia han sido sistemáticamente acosados por el gobierno de los Estados Unidos:

interrogados en aeropuertos, sometidos a agresivos cacheos y amenazas ilegales de cárcel inminente por parte de agentes de la ley, su equipo ha sido confiscado y sus servicios en la red han sido objeto de numerosas citaciones secretas. A Jacob no le amedrentan estas medidas y prosigue con sus múltiples batallas legales; erigido en ferviente defensor de la libertad de expresión, es una de las voces más elocuentes de WikiLeaks.

Andy Müller-Maguhn fue uno de los primeros miembros del Club del Caos Informático en Alemania, antiguo miembro y vocal del consejo.[6] Es uno de los cofundadores de EDRI (European Digital Rights/Derechos Digitales Europeos), una ONG pro derechos humanos en la era digital.[7] Durante los años 2000 a 2003, fue elegido por los usuarios europeos de internet como director europeo de ICANN (Corporación de Internet de Nombres y Números Asignados), responsable de la política mundial que rige los designios de los «nombres y los números» en la red.[8] Está especializado en telecomunicaciones y otros sistemas de vigilancia, trabaja como periodista en la industria de la vigilancia con su proyecto wiki, buggedplanet.info.[9] Andy trabaja en comunicación criptográfica y fundó con otros compañeros una empresa llamada Cryptophone, que comercializa dispositivos seguros de comunicación de voz y ofrece asesoría estratégica en el contexto de la arquitectura de red.[10]

Jérémie Zimmerman es el cofundador y portavoz del grupo civil de apoyo La Quadrature du Net, la organización europea más destacada en el ejercicio de la defensa del derecho al anonimato en la red y en la concienciación sobre la existencia de ataques normativos a las libertades virtuales. [11] Jérémie trabaja para construir herramientas que permitan la participación de los usuarios en el debate público e intentar así cambiar las cosas. Está tremendamente implicado en las guerras de derechos de autor y en el debate sobre la neutralidad de la red y otras cuestiones reglamentarias cruciales para el futuro de internet libre. Recientemente, su grupo La Quadrature du Net consiguió un hito histórico en la política europea, dirigiendo con éxito una campaña pública de rechazo al Acuerdo Comercial de la Lucha contra la Falsificación (ACTA), en el Parlamento Europeo. Poco después de participar en el debate que sienta las bases de este libro, Jérémie fue abordado por dos agentes del FBI cuando abandonaba Estados Unidos e interrogado acerca de WikiLeaks.

Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella

En varios de los puntos abordados en el siguiente debate se mencionan eventos recientes de la historia de WikiLeaks y

sus últimas acciones editoriales. Dado que estas citas pueden resultar confusas para los lectores no familiarizados con la historia de WikiLeaks, éstas se resumen en el presente apartado.

Es misión de WikiLeaks recibir información de denunciantes, hacerla pública y luego defenderse frente a los subsiguientes ataques políticos y legales. Los intentos de boicotear las filtraciones de WikiLeaks se han convertido en algo rutinario para las corporaciones y Estados poderosos, y como editorial de último recurso que es, ésta es una de las penurias que WikiLeaks está dispuesta a afrontar.

En el año 2010, WikiLeaks sacó a la luz los documentos más controvertidos que había publicado hasta la fecha, revelando el abuso sistemático del secreto oficial en el ejército y el gobierno de los Estados Unidos. Estas publicaciones se conocen internacionalmente como *Collateral Murder* («Asesinato Colateral»), *The War logs* («Los documentos de la Guerra de Irak»), y *Cablegate* («Cables del Departamento de Estado Norteamericano»)[12]. La respuesta se traduce en el actual esfuerzo conjunto que ejerce el gobierno de los Estados Unidos y sus aliados para destruir WikiLeaks.

El gran jurado de WikiLeaks

Como consecuencia directa de las publicaciones de WikiLeaks, el gobierno de Estados Unidos inició una investigación criminal multiagencia sobre Julian Assange y el personal de WikiLeaks, sus partidarios y presuntos colaboradores. Un jurado indagatorio fue convocado en Alejandría, Virginia, con el apoyo del Departamento de Justicia y del FBI para estudiar si, a tenor de la Ley de Espionaje de 1917, existía la posibilidad de imputar cargos, incluido el de conspiración, a Julian Assange y sus partidarios. Los agentes americanos declararon que la investigación era «de una naturaleza y una magnitud sin precedentes». En los procesos de gran jurado no hay ningún juez o abogado defensor. Las audiencias del comité del congreso vienen escuchando desde entonces la propuesta por parte de algunos miembros del Congreso de Estados Unidos de que la Ley de Espionaje se utilice como herramienta para procesar a periodistas que «deliberadamente publiquen información confidencial», sugiriendo que el enfoque se institucionalice en el sistema de justicia americano.[13]

Hasta la fecha, la investigación de WikiLeaks continúa.[14] Distintas personas han sido legalmente obligadas a aportar pruebas. Los procedimientos judiciales en el caso de Bradley Manning, el soldado acusado de pasar información a WikiLeaks, revelan un archivo del FBI sobre la

investigación de WikiLeaks de más de 42.000 páginas, de las cuales ocho mil abordan el caso de Manning. Bradley Manning lleva detenido sin juicio más de 880 días. El relator especial de Naciones Unidas para la Tortura, Juan Méndez, descubrió y reconoció formalmente que Bradley Manning había sido tratado de modo cruel e inhumano, hasta el punto de poder catalogar el maltrato de tortura.[15]

Peticiones de asesinato para Julian Assange y el equipo oficialmente reconocido de WikiLeaks

La investigación del gran jurado no es el único frente abierto contra WikiLeaks. En diciembre de 2012, a raíz de las filtraciones del asunto *Cablegate*, varios políticos plantearon enérgicamente el asesinato extrajudicial de Julian Assange, llegando a proponer la utilización de reactores no tripulados. Los senadores norteamericanos calificaron a WikiLeaks de «organización terrorista» tildando a Assange de «terrorista tecnológico» y «combatiente enemigo» involucrado en la «guerra cibernética».[16]

Un sólido equipo constituido por 120 personas del Pentágono bajo el sobrenombre de Cuerpo Especial WikiLeaks fue creado inmediatamente antes de que salieran a la luz los documentos de la guerra de Irak y el *Cablegate*, con el fin de «adoptar medidas» contra WikiLeaks. Es de

dominio público que existen cuerpos especiales similares en el FBI, la CIA y el Departamento de Estado norteamericano, todos operativos a día de hoy.[17]

Censura directa

En un acto de censura a una agencia periodística sin precedentes, el gobierno de Estados Unidos presionó a los servidores de internet para que dejaran de dar servicio a Wikileaks.org. El 1 de diciembre de 2010, Amazon eliminó a WikiLeaks de sus servidores de almacenamiento y el 2 de diciembre, el servidor DNS (sistema de nombres de dominio) asignado al dominio de Wikileaks.org fue atacado. WikiLeaks se mantuvo en la red durante este periodo gracias a la creación masiva de *mirrors* (espejos), por medio de los cuales miles de seguidores de WikiLeaks copiaban el sitio web y alojaban su propia versión distribuyendo las direcciones IP a través de las redes sociales.[18]

La Administración Obama ordenó a los empleados federales que mantuvieran como «clasificado» el material filtrado por WikiLeaks —pese a que esta información estaba siendo publicada por algunas de las agencias de noticias más importantes del mundo, incluidos los diarios *The New York Times* y *The Guardian*—. Los empleados recibieron la consigna de que el acceso al material, ya fuera a través de

Wikileaks.org o de *The New York Times*, se consideraría violación de la seguridad.[19] Tanto las agencias gubernamentales como la Biblioteca del Congreso, el Departamento de Comercio y el Ejército de Estados Unidos bloquearon el acceso al material de WikiLeaks a través de sus respectivas redes. La prohibición no se limitaba únicamente al sector público. Los empleados del gobierno de Estados Unidos advirtieron a las instituciones académicas de que los estudiantes que quisieran hacer carrera en el sector público debían evitar todo contacto con las informaciones reveladas por WikiLeaks en sus investigaciones y en su actividad en la red.

Censura financiera: el bloqueo bancario

WikiLeaks se financia con las donaciones de sus seguidores. En diciembre de 2010 las instituciones bancarias y financieras, incluidas VISA, MasterCard, Paypal y el Bank of America, cedieron a las presiones oficiosas de Estados Unidos y empezaron a denegar servicios financieros a WikiLeaks. Bloquearon las transferencias bancarias y todas las donaciones efectuadas con las principales tarjeras de crédito. Dado que todas ellas son instituciones norteamericanas, su ubicuidad en el mundo financiero derivó en que a muchos donantes, tanto de América como del resto

del mundo, se les denegó la opción de enviar dinero a WikiLeaks para financiar su actividad periodística.

El bloqueo bancario, así se le conoce, se está llevando a cabo al margen de procedimiento judicial o administrativo alguno, y continúa vigente a día de hoy. WikiLeaks tiene importantes causas abiertas en distintas jurisdicciones del mundo para romper este bloqueo; con algunas victorias preliminares, los procesos judiciales siguen su curso. Mientras tanto WikiLeaks, carente de ingresos y con elevados costes, opera con fondos de reserva desde hace casi dos años.

El bloqueo bancario es una reafirmación del poder que controla las transacciones económicas entre terceros. Menoscaba sin cortapisas las libertades económicas de los individuos. Va incluso más allá: la amenaza existencial que representa para WikiLeaks encarna una nueva y preocupante forma de censura económica global.[20]

Algunas personas supuestamente asociadas con WikiLeaks, así como sus seguidores y el propio personal de la organización, han tenido misteriosos incidentes con sus cuentas bancarias que incluyen desde problemas con sus datos hasta el cierre definitivo de sus cuentas.

Acoso a Jacob Appelbaum y Jérémie Zimmermann

El 17 de Julio de 2012, Julian Assange fue elegido para dar una charla en la conferencia «Hackers on Planet Earth (HOPE)» (Hackers en el Planeta Tierra), celebrada en la ciudad de Nueva York. Canceló su intervención y Jacob Appelbaum participó en su lugar. Desde su aparición, las agencias de orden público han llevado a cabo una campaña de acoso y derribo contra Appelbaum y las personas de su entorno. Desde entonces Appelbaum es objeto de frecuentes detenciones e investigaciones, denegándosele cualquier tipo de asistencia jurídica y siendo sometido a interrogatorios en la aduana cada vez que entra y sale de Estados Unidos. Su equipo ha sido confiscado y sus derechos violados en repetidas ocasiones bajo la amenaza de acciones similares futuras. En esta persecución han participado docenas de agencias gubernamentales, desde el Departamento de Seguridad Interna, Inmigración y Aduanas, al Ejército norteamericano. Las detenciones incluían además la prohibición del acceso al cuarto de baño como método de presión. Appelbaum no ha sido nunca acusado formalmente ni ha recibido explicación alguna por parte del gobierno sobre las razones del acoso que viene padeciendo.[21]

A mediados de junio del año 2011, cuando se disponía a embarcar en un avión en el aeropuerto Dulles de Washington, Jérémie Zimmermann fue abordado por dos hombres que se identificaron como agentes del FBI. Estos agentes le hicieron preguntas sobre WikiLeaks y le

amenazaron con detenerle y encarcelarle.

Appelbaum y Zimmermann se encuentran en la lista de amigos, seguidores o presuntos colaboradores de Julian Assange que han sido objeto del acoso y vigilancia por parte de agencias gubernamentales norteamericanas, una lista que incluye a abogados y periodistas que se limitan a hacer su trabajo.

Confiscación sin mandamiento judicial de archivos electrónicos y «la citación de Twitter»

El 14 de diciembre de 2010, Twitter recibió una «citación administrativa» del Departamento de Justicia de Estados Unidos en la que se le instaba a revelar información relacionada con la investigación abierta sobre WikiLeaks. La citación se presentó al amparo del artículo USC2703 apartado (d) de la *Stored Wire and Electronic Communications and Transactional Records Access*, dentro de la Ley de Privacidad de las Comunicaciones Electrónicas, comúnmente conocida como la «orden 2703(d)». El gobierno estadounidense, a tenor de esta ley, se declara competente para exigir la revelación de comunicaciones electrónicas privadas sin necesidad de que un juez dicte una orden de registro, sentando así las bases legales para sortear las protecciones conferidas por la Cuarta Enmienda frente al

registro y embargo arbitrarios.

La citación requería nombres de usuario, correos electrónicos, direcciones IP, números de teléfono, cuentas bancarias y números de tarjetas asociados con cuentas y personas presuntamente relacionadas con WikiLeaks, incluidos los de sus seguidores Jacob Appelbaum, la parlamentaria islandesa Birgitta Jónsdóttir, y el empresario holandés y pionero de internet Rop Gonggrijp. Según los términos de la citación, Twitter no podía bajo ningún concepto comunicar su existencia a los interesados. Twitter recurrió con éxito esta prohibición y consiguió que se le reconociera el derecho de informar a estas personas de la confiscación de sus archivos. Twitter se lo notificó el día 5 de enero de 2011.

El 26 de enero de 2011, Appelbaum, Jónsdóttir y Gonggrijp, representados por Kecker y Van Nest, La Unión Americana de Libertades Civiles (ACLU) y La Fundación Fronteras Electrónicas (EFF), convocaron a sus respectivos abogados para interponer un recurso de nulidad contra dicha orden. A este caso se le conoce como «la citación de Twitter».[22] Por su parte, el abogado de Appelbaum presentó un nuevo recurso en el que solicitaba la desclasificación de los expedientes judiciales que revelaban los intentos gubernamentales de recabar información privada de Twitter y otras compañías que podían haber sido objeto de estas mismas presiones por parte del gobierno

estadounidense. Ambos recursos fueron desestimados por un magistrado de Estados Unidos el día 11 de marzo de 2011. Los demandantes apelaron esta resolución.

El 9 de octubre de 2011, el diario *Wall Street Journal* reveló que el servidor californiano de correo Sonic.net había recibido una citación similar solicitando información de Appelbaum. Sonic recurrió la orden ante un tribunal y perdió, pero obtuvo el permiso para comunicar a Appelbaum que había sido obligada a remitir información sobre su persona. El diario *Wall Street Journal* también apuntaba que Google se encontraba en la misma situación, si bien no mencionaba si el gigante había presentado recurso alguno al respecto.[23]

El 10 de noviembre de 2011, un juez federal de primera instancia del distrito de Alejandría, Virginia, se pronunció en contra de Appelbaum, Jónsdóttir y Gonggrijp al dictaminar que Twitter debía suministrar la información de sus cuentas al Departamento de Justicia.[24] El 20 de enero de 2012 los demandantes recurrieron tratando de impugnar la resolución de noviembre que desestimaba «la desclasificación o publicación de la lista de citaciones que pudieran haberse enviado a terceras empresas, además de a Twitter, así como los recursos y autos relacionados con las mismas».[25] Hasta la fecha el caso sigue abierto.

Mayor comunicación versus mayor vigilancia

JULIAN

Si nos remontamos a los primeros años de la década de los noventa, cuando el movimiento criptopunk alcanzó su apogeo en respuesta a la prohibición de la criptografía por parte de los Estados, mucha gente tenía la mirada puesta en el poder de internet para ofrecer comunicaciones libres y sin la censura de los medios generalistas. Sin embargo los criptopunks siempre vieron que, en combinación con esto, existía también el poder para vigilar en tiempo real todas las comunicaciones que se efectuaban. Ahora contamos con mayores comunicaciones frente a una mayor vigilancia. Mayor comunicación quiere decir que todos tenemos un plus de libertad con respecto a aquellos que intentan controlar las ideas y fabricar el consenso, y mayor vigilancia significa justamente lo contrario.

La vigilancia es a día de hoy mucho más evidente que la

vigilancia del pasado, ejercida en bloque por los americanos, británicos, rusos y otros gobiernos contados como el sueco y el francés. Ahora la ejerce todo el mundo, y prácticamente todos los países, a resultas de la comercialización de la vigilancia masiva. Y se ha convertido en una vigilancia totalizadora, pues la gente expone en internet todas sus ideas políticas, todas las comunicaciones que establece con familiares y amigos. De modo que no se trata sólo de que haya aumentado la vigilancia en las comunicaciones que ya existían; el caso es que ahora la comunicación es mucho mayor; se ha producido un incremento en los tipos de comunicación. Todos estos nuevos tipos de comunicación que en el pasado habrían pertenecido a la esfera privada de las personas ahora están siendo interceptados masivamente.

Se está librando una batalla entre el poder de esta información recopilada por infiltrados, Estados de información en la sombra que están empezando a desarrollarse, confundiéndose unos con otros, desarrollando conexiones entre sí y con el sector privado, y el creciente volumen de mortales que utilizan internet como una herramienta común de expresión de la humanidad.

Quiero reflexionar sobre cómo presentamos nuestras ideas. El gran problema se me plantea, al estar tan involucrado en la vigilancia estatal y comprender cómo se ha desarrollado la industria de seguridad transnacional a lo largo de los últimos veinte años, es que estoy demasiado

familiarizado con ello y me cuesta verlo desde un punto de vista generalizado. Sin embargo, ahora nuestro mundo pertenece a la colectividad, porque todo el mundo ha depositado el núcleo interno de sus vidas en internet. Es nuestro deber comunicar de alguna manera lo que sabemos, ahora que todavía podemos.

ANDY

Yo propongo no plantearlo desde el punto de vista del ciudadano sino desde el de aquellos que manejan el poder. El otro día estaba en esta extraña conferencia en Washington y me topé con unos tíos que llevaban una chapa de la embajada alemana. Me acerqué a ellos y les dije: «Anda, sois de la Embajada alemana»; y ellos me respondieron: «Ah, no exactamente de la Embajada, somos de cerca de Múnich». Al final resultaron ser del servicio de inteligencia y en bufé de la cena les hice unas cuantas preguntas: «Entonces ¿cuál es el objetivo del secreto?». Ellos me contestaron: «Bueno, se trata de ralentizar los procesos para poder controlarlos mejor». Ése es el objetivo de este tipo de trabajo de inteligencia, ralentizar un proceso quitándole a la gente la capacidad de entenderlo. Declarar cosas secretas significa que limitas la cantidad de gente que las conoce y, por ende, la capacidad de afectar al proceso mismo.

Si observas internet desde la perspectiva de las

personas que están en el poder, entonces los últimos años han sido aterradores. Ven internet como una enfermedad que afecta a su capacidad de definir la realidad, de definir lo que está pasando, lo cual se utiliza a posteriori para fijar lo que la gente sabe acerca de lo que está pasando y su capacidad para interactuar con ello. Si te fijas en, pongamos, Arabia Saudí, donde por algún accidente histórico los líderes religiosos y la fuerza mayoritaria son los mismos, su interés por el cambio es cero. Cero menos cinco, puede. Ven internet como una enfermedad y preguntan a sus asesores: «¿Tenéis el remedio para acabar con esto? Necesitamos inmunizarnos si afecta a nuestro país, si esta historia de internet llega hasta nosotros». Y la respuesta es la vigilancia masiva: «Necesitamos controlarlo totalmente, necesitamos filtrar, necesitamos saber todo lo que hacen». Y eso es lo que ha sucedido en los últimos veinte años. Se hizo una inversión masiva en vigilancia porque quienes ostentaban el poder temían que internet afectara su estilo de gobierno.

JULIAN

Sin embargo, pese a esta vigilancia masiva, la comunicación masiva ha derivado en que millones de personas son capaces de conseguir un rápido consenso. Si puedes pasar tan rápidamente de una posición normal a una nueva postura de consenso masivo, entonces, cuando el Estado consiga detectar este desarrollo, será demasiado

tarde para formular una respuesta efectiva.

Dicho esto, en el año 2008 hubo una protesta orquestada a través de Facebook en El Cairo. Ésta sorprendió al gobierno de Mubarak y como consecuencia, los organizadores de la protesta de Facebook fueron detenidos.[1] En el año 2011, en un manual considerado uno de los documentos más importantes utilizados en la revolución egipcia, la primera página y la última decían «no utilizar Twitter o Facebook para distribuir el manual».[2] Con todo, muchos egipcios utilizaron Twitter y Facebook. Sin embargo, la razón de que sobrevivieran se debe a que la revolución tuvo éxito. De no haber sido así, entonces esas personas habrían estado en una posición tremendamente delicada. Y no olvidemos que poco antes el presidente Mubarak había cortado el acceso a internet en Egipto. De hecho, todavía se cuestiona si la censura de internet facilitó la revolución o, por el contrario, la perjudicó. Algunos dicen que la benefició, pues la gente se vio obligada a salir a la calle para enterarse de lo que estaba ocurriendo, y una vez estás en la calle, estás en la calle. Yestas personas se vieron directamente afectadas porque sus teléfonos móviles e internet no funcionaban.

De modo que si va a tener éxito, tiene que haber una masa crítica, debe ocurrir rápido, y necesita ganar, porque si no gana, entonces la misma infraestructura que permite desarrollar un consenso rápido se utilizará para detectar y

marginar a todos aquellos dedicados a sembrar el consenso.

Y eso pasó en Egipto, país que, en efecto, era un aliado de Estados Unidos, pero que no pertenecía a la alianza de inteligencia de países angloparlantes conformada por Estados Unidos, Reino Unido, Australia y Canadá. Ahora, imaginemos por un momento que la revolución de Egipto se planteara en Estados Unidos, ¿Qué pasaría con Facebook y Twitter? Serían tomados por el Estado. Y si la revolución no triunfara, acabarían siendo espiados, como ahora, por la CIA y el FBI para recabar información sobre los principales promotores de la revuelta.

JÉRÉMIE

Es difícil disociar la vigilancia del control. Necesitamos abordar ambos. Eso es lo que a mí más me preocupa, el control de internet, ya sea por los gobiernos o por compañías privadas.

JACOB

Creo que está bastante claro que la censura es un producto derivado de la vigilancia en general, tanto en el caso de la autocensura como en el de la censura técnica, y creo que un modo importante de transmitir esto a las personas de a pie es hacerlo de una manera no técnica. Por ejemplo, si construyéramos carreteras tal como construimos internet, cada carretera tendría cámaras de vigilancia y

micrófonos a los que nadie, excepto la policía o alguien que se hiciera pasar con éxito por policía, podría acceder.

JULIAN

Ya están en ello, Jake, en el Reino Unido.

JACOB

Cuando construyes una carretera no se exige que cada milímetro de la misma esté controlado por un perfecto sistema de vigilancia sólo disponible para un grupo selecto de personas. Explicar al ciudadano de a pie que ése es el modo en que se están construyendo las carreteras en internet y luego pedirles que utilicen dichas carreteras... Eso es algo que la gente común puede relacionar con el momento en que se dan cuenta de que los constructores originales no siempre son aquellos que ejercen el control.

ANDY

Pero alguna gente ni siquiera construye carreteras. Plantan un jardín ahí fuera e invitan a desnudarse a todo hijo de vecino. Me refiero a Facebook, claro, un modelo de negocio orientado a que la gente se sienta cómoda y revele su información.

JACOB

Exacto. Antes se recompensaba a aquellos que

colaboraban con la Stasi (el antiguo Ministerio para la Seguridad del Estado de Alemania del Este), y ahora se premia a aquellos que participan en Facebook. La diferencia es que en Facebook se les compensa con créditos sociales —acostarse con tu vecino/a— en lugar de pagarles directamente. Y es importante relacionarlo únicamente con el aspecto humano, porque no se trata de tecnología, se trata de controlar a través de la vigilancia. En cierto sentido es el perfecto Panóptico.[3]

JULIAN

A mí me interesa mucho la filosofía de la técnica. Técnica no significa únicamente un pedazo de tecnología, sino que significa, digamos, un consenso mayoritario en un consejo, o la estructura de un parlamento, es la interacción sistematizada. Por poner un ejemplo, diría que los sistemas feudales provienen fundamentalmente de la técnica de los molinos. Es decir, una vez contabas con molinos centralizados que requerían enormes inversiones y que no podían escapar del control físico, entonces lo natural era que, como consecuencia, acabaras teniendo relaciones feudales. Con el paso del tiempo, parece que hemos desarrollado técnicas cada vez más sofisticadas. Algunas de estas técnicas pueden democratizarse; pueden llegar a todos y cada uno de nosotros. Pero la mayoría, dada su complejidad, son técnicas que se crean gracias a

organizaciones estrechamente interconectadas como Intel Corporation. Tal vez la tendencia subyacente de la técnica consista en atravesar sus diversas fases: técnica de descubrimiento, técnica de centralización y técnica de democratización, cada vez que una generación formada aprende cómo hacerlo. Sin embargo, creo que la tendencia general de la técnica es la de centralizar el control en aquellos que controlan los recursos físicos de dicha técnica.

Algo parecido a un fabricante de semiconductores, creo yo, el máximo exponente de esto, donde necesitas desde la orden de que el aire mismo sea puro hasta una planta de construcción con miles de personas obligadas a llevar redecilla para proteger del proceso de manufactura hasta el último resquicio de piel, hasta el último pelo de la cabeza, un proceso polifásico extremadamente complicado. Y hay literalmente millones de horas de conocimiento investigador en manos del fabricante de semiconductores. Si éstos son populares, que lo son, y conforman los cimientos de internet, entonces la manufactura de semiconductores está codificada en el seno de la liberación de internet. Y codificada en la manufactura de semiconductores está la habilidad de quienquiera que detente el control físico del fabricante de semiconductores para extraer enormes concesiones.

De modo que podemos afirmar que en la sustentación de la revolución tecnológica de las comunicaciones —y la

libertad que hemos conseguido a partir de ésta— radica la actual economía neoliberal, transnacional y globalizada de mercado. De hecho, es el pico más alto de la misma. Lo mejor, en lo que a logros tecnológicos se refiere, que la actual economía global y neoliberal puede producir. Internet se basa en interacciones comerciales extremadamente complejas entre fabricantes de fibra óptica, fabricantes de semiconductores, compañías mineras que extraen el material necesario para ello, y todos los lubricantes financieros que hacen posible que este negocio se consolide, tribunales que hacen valer las leyes de propiedad privada y demás. Así que se trata en realidad de la cúspide de la pirámide de todo el sistema neoliberal.

ANDY

Sobre el tema de la técnica, cuando Johannes Gutenberg inventó la imprenta, ésta se prohibió oficialmente en algunas partes de Alemania y ése fue el modo en que se propagó por todo el país, pues cuando se prohibía en un área, se trasladaba a otra jurisdicción.[4] No he estudiado el caso en detalle pero, por lo que sé, tuvo sus divergencias con la Iglesia católica al romper el monopolio que ésta ostentaba en la impresión de libros, y cada vez que acababan teniendo problemas legales, se mudaban a otro sitio donde la imprenta no estuviera prohibida. En cierto sentido, esto ayudó a su propagación.

Internet fue, en mi opinión, sutilmente diferente porque, por un lado, tenías las máquinas que podías utilizar como una planta de producción, incluso la Commodore 64 lo era en cierta forma, si bien la mayoría de la gente la utilizaba para otros fines.

JULIAN

Así que, por pequeña que fuera la máquina que tuvieras podías usar tu propio software.

ANDY

Sí, y la podías utilizar para distribuir ideas. Sin embargo, por otro lado, desde una perspectiva filosófica, como dijo John Gilmore (uno de los fundadores de la Fundación Norteamericana de Fronteras Electrónicas), a principios de la década de los noventa, cuando internet consiguió un alcance global: «La red interpreta la censura como un perjuicio y la circunvala».[5] Hoy sabemos que la afirmación era una mezcla de interpretación técnica combinada con una perspectiva de impacto optimista, algo entre una quimera y una profecía susceptible de cumplirse.

JULIAN

Pero así fue en el caso de Usenet, un sistema de correo electrónico «muchos a muchos», por así decirlo, que se inició hace unos treinta años. Para explicar Usenet de manera

simple, imaginad que no existe diferencia alguna entre los usuarios y los servidores y que cada persona dirige su propio servidor Usenet. Escribes algo y se lo das a una o dos personas. Ellas (automáticamente) comprueban si ya lo tienen. Si aún no lo han recibido lo toman y se lo pasan a todos aquellos con los que están conectados. Y como resultado el mensaje acaba llegando a todos, y todos obtienen eventualmente una copia. Si algún usuario está involucrado en la censura el resto lo pasa por alto, no implica ningún cambio. El mensaje sigue propagándose a través de aquellos que no son censores. Gilmore hablaba sobre el uso de Usenet, no hablaba de internet. Tampoco hablaba de páginas web.

ANDY

Si bien lo que dices es técnicamente correcto, la interpretación de sus palabras y su impacto a largo plazo fue el de generar personas que se consideraban a sí mismas parte de internet. La gente decía «de acuerdo, hay censura, la sortearemos», mientras que el político que carecía de conocimientos técnicos pensaba «oh, mierda, hay una nueva tecnología que limita el control de la esfera de la información». Así que creo que Gilmore, sin duda uno de los precursores del movimiento criptopunk, hizo un gran trabajo al llevar las cosas en esta dirección, inspirando el modo cripto-anarquista de tener tu propia forma de comunicación

anónima sin temor a ser espiado.

JÉRÉMIE

Yo veo un matiz en eso que nosotros describimos como la propagación de la tecnología, porque en el caso del molino y la imprenta tenías que ver el artefacto físico para entender cómo funcionaba, mientras que ahora incorporamos un control cada vez mayor en la propia tecnología. El control está integrado. Si observas un ordenador moderno, en la mayoría de los casos, ni siquiera lo puedes abrir para conocer todos sus componentes. Y todos los componentes se encuentran a su vez en cajas diminutas, es imposible saber cómo funcionan.

ANDY

¿Por su complejidad?

JÉRÉMIE

Sí, por la complejidad y también porque no se tiene la intención de que la tecnología se comprenda. Tal es el caso de la tecnología patentada.[6] Cory Doctorow la define en una entrada de su blog titulada «La guerra a la computación de uso general».[7] Cuando un ordenador es una máquina genérica, puedes hacer de todo con él. Puedes procesar cualquier información como una «entrada» y transformarla en otra cosa como una «salida». Y sin embargo cada vez

construimos más dispositivos que, si bien son ordenadores de uso general, están restringidos a hacer las funciones limitadas de un GPS, o de un reproductor MP3 o de un teléfono móvil. Cada vez se fabrican más dispositivos que integran mecanismos de control para prohibir al usuario hacer cierto tipo de cosas.

JULIAN

El control se integra en los dispositivos para evitar que la gente los entienda o pueda utilizarlos de un modo distinto al originalmente pretendido por el fabricante, pero en la actualidad el problema es mucho peor, porque todos estos dispositivos están conectados a la red.

JÉRÉMIE

Cierto, pueden contener la función de monitorizar al usuario y su información. Ésta es la razón por la que el software libre es tan importante para una sociedad libre.

ANDY

Estoy totalmente de acuerdo en que necesitamos máquinas de uso general, pero esta mañana cuando trataba de volar hasta aquí desde Berlín, el avión abortó el despegue —es la primera vez que me ocurre algo así—. El avión se desplazó a un lado y el capitán dijo: «Damas y caballeros,

hemos tenido un fallo en el sistema eléctrico, así que hemos decidido parar y reiniciar el sistema». Y yo pensaba: «Oh, mierda, suena a reiniciar Windows, Control Alt, Delete... Tal vez, ¡funcione!». De modo que en realidad, no me molesta del todo la idea de tener una máquina que desempeñe una sola función en un avión, y que lo haga muy bien. Si estoy sentado en un aparato volador no quiero que los pilotos se distraigan jugando al Tetris, o con el Stuxnet o cualquier otra incidencia.[8]

JÉRÉMIE

El avión en sí mismo no procesa tus datos personales, no tiene ningún control sobre tu vida.

ANDY

Bueno, diría que una máquina que vuela sí tiene cierto control sobre mi vida, al menos durante un rato.

JACOB

Creo que el argumento de Cory también se explica mejor diciendo que no hay más coches, ni aviones, ni audífonos, sino ordenadores con cuatro ruedas, ordenadores con alas y ordenadores que mejoran tu audición. Y la cuestión, en parte, no es si son o no ordenadores con una sola función, sino si podemos verificar que efectivamente hacen aquello que dicen que hacen, y si entendemos si lo hacen

correctamente. La gente trata a menudo de argumentar que tienen el derecho a poner el candado y mantener el secreto acerca de estos dispositivos y, o bien fabrican ordenadores demasiado complejos, o dificultan legalmente el camino para entenderlos. Eso es algo realmente peligroso para la sociedad porque nosotros sabemos que la gente no siempre actúa en beneficio de todos. También sabemos que la gente comete errores —sin malicia—, así que echar la llave a este tipo de cosas es muy peligroso a distintos niveles, de los cuales el que seamos todos imperfectos no es un problema menor. Eso es un hecho. La capacidad para tener acceso a los planos de los sistemas que subyacen en nuestras vidas es parte del porqué el software libre es importante, pero también la razón que explica la importancia del hardware libre. Ello mejora nuestra capacidad de hacer libremente inversiones sostenibles tanto para mejorar los sistemas que utilizamos como para determinar si éstos funcionan correctamente.

Sin embargo, independientemente de la libertad, es importante entender estos sistemas, porque, de lo contrario, existe una tendencia generalizada a delegar en la autoridad, en personas que sí los conocen, o que son capaces de ejercer el control sobre los mismos pese a no comprender su esencia. Ello explica el bombo que se ha dado a la ciberguerra. Básicamente se debe a que una serie de personas que parecen ser *los señores de la guerra* empiezan

a hablar sobre tecnología como si la entendieran. Estos señores hablan a menudo de la guerra y ninguno de ellos, ni siquiera uno, habla sobre la ciber construcción de la paz, o de nada relacionado con la construcción de la paz. Hablan siempre de la guerra porque es su negocio, e intentan controlar los procesos tecnológicos y legales como medios para promover sus propios intereses. De modo que cuando no tenemos control sobre nuestra tecnología, dichas personas tratan de usarla para sus propios fines, concretamente para la guerra. Ésta es la receta para cosas tan escalofriantes como el Stuxnet, creo yo, aunque, por otro lado, también hay personas sensatas que, mientras Estados Unidos hace la guerra, sugieren que dichas tácticas evitarán de algún modo futuras guerras. Tal vez sea ése un argumento razonable para un país que no invade activamente otras naciones, pero difícil de creer en el contexto de una nación que en la actualidad está envuelta en numerosas invasiones simultáneas.

La militarización del ciberespacio

JULIAN

Ahora existe una militarización del ciberespacio, en el sentido de una ocupación militar. Cuando te comunicas a través de internet, cuando te comunicas a través del teléfono móvil, que ahora está entrelazado a la red, tus comunicaciones están siendo interceptadas por organizaciones de inteligencia militar. Es como tener un tanque en tu dormitorio. Es un soldado que se interpone entre tú y tu mujer cuando os enviáis mensajes. Todos estamos bajo una ley marcial en lo que respecta a nuestras comunicaciones, simplemente no podemos ver los tanques, pero están. Tanto es así que internet, que originalmente se planteaba como un espacio civil, se ha convertido en un espacio militarizado. Pero internet es nuestro espacio, porque todos lo usamos para comunicarnos entre nosotros, con nuestras familias, revelando lo más íntimo de nuestras

vidas. Así que, de hecho, nuestras vidas privadas han entrado en una zona militarizada. Es como tener un soldado debajo de la cama. Es una militarización de la vida civil.

JACOB

Justo antes de venir, me ofrecieron entrenar al equipo de estudiantes que integran el laboratorio de investigación para la seguridad y privacidad de la Universidad de Washington, para el concurso *Pacific Rim Collegiate Cyber Defense*. En el último minuto me pidieron que fuera su asesor. Hemos dedicado bastante tiempo a competir en una batalla cibernética donde SPAWAR, un brazo civil de la marina norteamericana que realiza pruebas de penetración basadas en maniobras ofensivas y defensivas de piratería informática, desempeñaba el rol del *Red Team* (equipo rojo). [1] Este equipo se dedica básicamente a atacar al resto de jugadores cuyos equipos tratan de defender los sistemas informáticos que les son asignados al principio de la batalla sin ningún tipo de información adicional. Uno no sabe el tipo de sistemas que tendrá que defender y ni siquiera está claro cómo se asignan los puntos al principio, por lo que sólo te queda hacerlo lo mejor posible y esperar.

JULIAN

¿Estás seguro de que se trata de un juego? Tal vez no sea ningún juego.

JACOB

No, te dan unos cuantos ordenadores y tienes que protegerlos, ellos irrumpen en el sistema y asumen el control. Es como la versión infantil de *Captura la Bandera* en una conferencia real de piratas informáticos o algo parecido, y es interesante porque estos tíos cuentan con un montón de herramientas, tienen software escrito.[2]

JULIAN

Pero entonces ¿qué sentido tiene desde la perspectiva de la Marina norteamericana?

JACOB

Bueno, en su caso se limitan a patrocinar el juego porque quieren empezar a construir los ciberguerreros del mañana y, para que veas un ejemplo, te he traído un bloc de notas de la CIA que confirma que, de hecho, se están dedicando a reclutar gente en este tipo de eventos. Había un tío llamado Charlie —Charlie de la CIA—, que ofrecía trabajo a los participantes diciéndoles que, si querían unirse a la CIA, ésta era una gran oportunidad para trabajar en el mundo real. Y la gente de SPAWAR estaba allí, y Microsoft estaba allí contratando personal. La idea era formar a toda esta gente, a todos estos equipos, para que saltaran al Campeonato Nacional y se convirtieran en ganadores y

«defendieran la nación», y luego fueran capaces de hacer piratería ofensiva como ciberguerreros y no sólo como ciberdefensores. Nosotros obtuvimos alrededor de 4.000 puntos en este juego, lo cual superaba la puntuación total de los equipos que quedaron en segundo, tercer y cuarto lugar. Obtuvimos mayor puntuación que la suma de las puntuaciones de todos ellos.

JULIAN

¡Bravo, bravo, bravo!

JACOB

El caso es que no me lo deben a mí, mi frase para motivarles era algo parecido a: «Eh, el tono siempre es más oscuro justo antes de que las cosas se pongan negras del todo». Personalmente, creo que no se me da muy bien el *coaching,* pero estos chicos son realmente buenos. El caso es que fue interesante porque todo se había dispuesto en los mismos términos que en una guerra real, de modo que te decían: «Eh, queremos oír vuestro grito de guerra». Y uno piensa: «Perdón ¿qué?». Te decían cosas así durante el almuerzo, cuando nos tomábamos un respiro en la defensa de nuestros sistemas. Todo estaba diseñado en términos de atacar sistemas, de guerra, ciberguerra y las cosas más alucinantes que te puedas imaginar al respecto. Y, curiosamente, aparte del equipo con que trabajaba, tuve la

sensación de que había mucha gente que sufría, porque no se les estaba enseñando *El arte de la guerra* —era más como la Copa de Sysadmin, gente responsable de mantener sistemas de computación— y era algo vergonzoso.[3] Fue una sensación muy rara porque te encontrabas con todas estas personas con bagaje bélico, que tenían la perspectiva de la guerra, pero que no enseñaban estrategia, y sólo se centraban en la retórica de defender estos sistemas, o en atacarlos, y tenían tanta guerra en el camino que trataban por todos los medios de enardecer el fervor patriótico de los participantes. No fomentaban el pensamiento creativo ni ningún tipo de marco para el análisis independiente; insertaban una nueva pieza en el engranaje mental de alguien que sigue órdenes por el bien de la nación. Jamás había vivido algo parecido. Me puso enfermo y a la mayor parte de mi equipo le costó un duro trabajo digerirlo e incluso tomarlo en serio.

JULIAN

¿Crees que así es la formación de la Marina estadounidense y que ahora sólo intentan aplicarla a otro dominio? ¿Es la creación de un Alto Cibercomando Norteamericano una decisión estratégica internacional tomada por los Estados Unidos?

ANDY

Como los nazis, que tenían esos campos juveniles donde formaban a los niños.

JACOB

Puedes decir eso porque eres alemán. No, no es así. La participación de la marina norteamericana se debe a que el gobierno estadounidense patrocina este tipo de eventos. Me pidieron que entrenara al equipo porque necesitaban que alguien lo hiciera, y accedí sólo porque me caía bien el equipo, esos chicos universitarios. Pero en realidad lo que es evidente es que el gobierno norteamericano está tratando de conseguir gente y lo intentan por la vía del nacionalismo. Es realmente raro estar en un evento como ése porque, por un lado, está bien ser capaz de saber cómo mantener a salvo tu sistema, y es bueno entender la infraestructura de la que dependen nuestras vidas; pero por otro, ellos no intentaban convencer a la gente para que la entendieran, sino más bien trataban de exaltar su fervor patriótico para que fueran felices haciendo este tipo de trabajo.

ANDY

Desafortunadamente, el interés de Estados Unidos por mantener los sistemas seguros es totalmente limitado, pues quieren que los sistemas sean vulnerables para poder asumir el control. El enfoque para controlar la criptografía a nivel

mundial nunca ha llegado tan lejos como cuando Estados Unidos empezó a ejercer presión en 1998, cuando el subsecretario estadounidense de comercio internacional, David Aarons, dio la vuelta al mundo abogando en su discurso por el acceso del gobierno a las claves cifradas de todos los ciudadanos.[4] No obstante, la criptografía todavía se gestiona como las llamadas tecnologías de doble uso y, según lo establecido en el denominado Acuerdo de Wassenaar, su exportación en forma de productos de consumo final a muchos países está limitada por ley.[5]

Esto puede parecer razonable en la tesitura de declarar «malos» a algunos países y sus acciones, pero sin embargo revela hasta qué punto se aplica un doble rasero, porque hasta la fecha, la tecnología de vigilancia de las telecomunicaciones no se ha visto limitada por controles de exportación.[6]

JULIAN

Andy, tú llevas años diseñando teléfonos criptográficos. ¿Qué tipo de vigilancia masiva se está aplicando a las telecomunicaciones? Dime, ¿cuál es la situación en lo que respecta a los servicios de inteligencia y la industria de vigilancia masiva?

ANDY

Almacenamiento masivo, que no es otra cosa que

almacenar todas las telecomunicaciones, todas las llamadas de voz, todo el tráfico de datos, cualquier modo en que los grupos consumen el Short Message Service (SMS o servicio de mensajes cortos), así como las conexiones a internet, limitadas en ocasiones al correo electrónico. Si comparas el presupuesto militar con los costes que comportan la vigilancia y los ciberguerreros, los sistemas armamentísticos ordinarios cuestan muchísimo más dinero. Los ciberguerreros o la vigilancia masiva son súper baratos en comparación con lo que cuesta un solo avión. Un avión militar te cuesta alrededor de...

JULIAN

Unos cien millones de dólares.

ANDY

Y el almacenamiento es cada año más barato. De hecho, en su día hicimos las cuentas en el Club del Caos Informático: puedes conseguir un buen almacenamiento en cuanto a calidad de voz de todas las llamadas telefónicas efectuadas en Alemania anualmente por cerca de 30 millones de euros, gastos administrativos incluidos, de modo que el almacenamiento puro cuesta alrededor de ocho millones de euros.[7]

JULIAN

E incluso existen compañías como VASTech en

Sudáfrica que están vendiendo estos sistemas por diez millones de dólares al año.[8] «Interceptaremos todas sus llamadas, almacenaremos todas las llamadas interceptadas en masa.» El hecho es que en los últimos años se ha producido un viraje en el planteamiento, se ha pasado de interceptar todo aquello que pasaba de un país a otro, seleccionando cuidadosamente a las personas concretas que querían espiar y asignándolas a seres humanos, a lo que hacen ahora: interceptar y almacenar todo permanentemente.

ANDY

Para explicar la historia a grosso modo, en los viejos tiempos se designaba a una persona como objetivo en función de su estatus diplomático, la compañía en que trabajaba, o bien porque fuera sospechoso de hacer algo o estuviera en contacto con gente que sí había hecho algo, y entonces se aplicaban las medidas de vigilancia pertinentes sobre esa persona concreta. Hoy día resulta mucho más eficiente decir: «Lo tomamos todo y ya lo resolveremos más tarde». De modo que cuentan con un almacenamiento a largo plazo. Y la mejor manera de describir estos dos capítulos de la industria es con el enfoque «táctico» y el enfoque «estratégico». Táctico significa: en este preciso momento, en esta reunión, vamos a colocar micrófonos ocultos en este lugar, necesitamos introducir a alguien con un micrófono en la chaqueta, o sistemas de vigilancia GSM

(Sistema Global para Comunicaciones Móviles) instalados en el coche, capaces de interceptar lo que la gente dice en el momento, sin necesidad de interferir con un el operador de red, sin necesidad de pedir una orden de registro ni nada parecido, sin necesidad de procedimientos legales. Hacerlo y listo. Sin embargo, el enfoque estratégico es hacerlo por defecto, limitarse a grabar todo y resolverlo después por medio de sistemas analíticos.

JULIAN

Entonces, la interceptación estratégica consiste en confiscar todo cuanto registra un satélite de telecomunicaciones, y hacerlo a través de un cable de fibra óptica.

ANDY

Porque nunca sabes cuando alguien se convierte en sospechoso.

JACOB

Estados Unidos vivió el caso NSA AT&T, y un segundo caso: Hepting v. AT&T. En Folson, California, Mark Klein, antiguo técnico del gigante de las comunicaciones AT&T, reveló que la NSA, la Agencia de Seguridad Nacional estadounidense, estaba almacenando toda la información que la compañía AT&T les proporcionaba acerca de sus

clientes. Fue una compra al por mayor: datos y llamadas de voz. Así que ahora hemos sabido que cada vez que yo cogía el teléfono o me conectaba a internet en San Francisco durante el periodo al que se refería Mark Klein, la Agencia de Seguridad Nacional, en suelo estadounidense y en contra de los ciudadanos estadounidenses, se estaba quedando con todo.[9] Estoy francamente convencido de que han usado toda esa información interceptada en las investigaciones que han llevado a cabo en contra de muchas personas en Estados Unidos, lo cual plantea un sinfín de interesantes cuestiones constitucionales, porque ellos se quedan con esta información para siempre.

JÉRÉMIE

Tenemos también el ejemplo de Eagle, el sistema vendido por la compañía francesa Amesys que posteriormente se vendió a la Libia de Gadafi, y en cuyo documento comercial estaba escrito: «Mecanismo de interceptación a escala nacional». Es una gran caja que colocas en alguna parte y que te permite escuchar todas las comunicaciones de tu gente.[10]

JULIAN

Hace diez años esto se veía como una fantasía, como algo en lo que sólo unos cuantos paranoicos creían, pero en la actualidad los costes de la interceptación masiva se han

reducido hasta el punto de que un país como Libia, con recursos relativamente escasos, lo estaba haciendo con tecnología francesa. De hecho, la mayoría de los países están ya ahí en términos de interceptación real. Sin duda la eficiencia en la comprensión y en la respuesta a lo que está siendo interceptado y almacenado será el gran paso siguiente. Ahora en muchos países tenemos interceptación estratégica de todo el tráfico de comunicaciones que entran y salen del país, pero implicarse en acciones subsiguientes, como bloquear automáticamente cuentas bancarias, o desplegar a la policía, marginar a ciertos grupos, o emancipar a otros, es todavía algo que está por llegar. Siemens vende una plataforma a las agencias de inteligencia que, de hecho, produce acciones automáticas. De tal modo que cuando el objetivo A se encuentra a cierto número de metros del objetivo B según los registros de intercepción móvil, y el objetivo A recibe un correo electrónico mencionando algo —una palabra clave—, entonces se activa la acción. Está al caer.

Combatir la vigilancia total con las leyes del hombre

JÉRÉMIE

Así que ahora es un hecho que la tecnología posibilita la vigilancia total de las comunicaciones. Y luego está la otra cara de esa moneda, que es qué hacemos con ella. Podríamos admitir que para todo lo que tú llamas vigilancia táctica existen algunos usos legítimos —cabe que investigadores que persiguen a chicos malos y sus redes, bajo la supervisión de la autoridad judicial, necesiten utilizar este tipo de herramientas—, pero la pregunta es dónde trazar la línea para esta supervisión judicial, dónde trazar la línea para el control que los ciudadanos pueden ejercer sobre el uso de dichas tecnologías. Esto es un tema político. Cuando entramos en este tipo de asuntos, te encuentras con políticos a los que se les pide que firmen algo sin entender la tecnología subyacente, y creo que aquí es donde nosotros, como ciudadanos, tenemos un papel, no sólo el de explicar

cómo funciona la tecnología en toda su extensión, a los políticos incluidos, sino también el de meter baza en los debates políticos que se suscitan en torno al uso de dichas tecnologías. Me consta que en Alemania hubo un movimiento masivo en contra de la retención generalizada de datos que derivó en la anulación de la Ley de Retención de Datos por parte del Tribunal Constitucional.[1] Actualmente se está debatiendo en la Unión Europea la posibilidad de revisar la Directiva sobre retención de datos.[2]

ANDY

Estás describiendo la teoría de Estado democrático que, por supuesto, necesita identificar a los chicos malos de aquí y allá, y escuchar sus llamadas atendiendo a una resolución judicial ponderada para garantizar que se hace de la manera adecuada. El problema de esto es que las autoridades deben actuar de acuerdo con la ley. Si no lo hacen, entonces ¿para qué sirven? En concreto, con este enfoque estratégico, los Estados democráticos europeos están comprando en masa máquinas que precisamente les permiten actuar fuera de la ley en lo que respecta a la interceptación, pues no necesitan una resolución judicial, se limitan a encender y espiar, y esta tecnología no puede ser controlada.

JULIAN

¿Pero no creéis que existen dos enfoques para afrontar

la vigilancia masiva de los Estados: las leyes de la física y las leyes del hombre? El primero consiste en usar las leyes de la física para construir dispositivos que prevengan la interceptación. El otro es para poner en práctica controles democráticos a través de leyes que garanticen la protección de los ciudadanos aplicando procesos que regulen la responsabilidad de los Estados. Sin embargo la interceptación estratégica no entra en este marco, no puede ser coartada de manera significativa por normas legales. La interceptación estratégica consiste en interceptar a todos, independientemente de que sean inocentes o culpables. Debemos recordar que ése es el fin del sistema que lleva a cabo dicha vigilancia. Siempre existirá una falta de voluntad política para desenmascarar el espionaje de los Estados. Y la tecnología es intrínsecamente tan compleja, y su uso es en la práctica tan secreto, que no puede existir una supervisión democrática de peso.

ANDY

O te dedicas a espiar a tu propio parlamento.

JULIAN

Eso son excusas —la mafia y la inteligencia exterior—, son excusas que la gente aceptará para erigir un sistema de este tipo.

JACOB

Los cuatro jinetes del *Info-Apocalipsis*: pornografía infantil, terrorismo, blanqueo de dinero y la guerra a ciertas drogas.

JULIAN

Una vez erigida esta vigilancia, dado que es compleja, dado que está diseñada para operar en secreto, ¿no es cierto que no puede ser regulada por la política? Creo que, salvo en el caso de naciones muy pequeñas como Islandia, a menos que se den condiciones revolucionarias, es sencillamente imposible controlar la interceptación masiva con legislación y política. No va a suceder. Es demasiado barato y demasiado fácil sortear la responsabilidad política y llevar a efecto la interceptación. Los suecos aprobaron una ley de interceptación en el año 2008, conocida como la Fra-lagen (ley FRA), por la que la agencia de inteligencia de señales sueca, conocida como la FRA, podía legalmente interceptar en masa todas las comunicaciones del país, y remitírselas a Estados Unidos, con algunas salvedades legales.[3] Pero ¿cómo se pueden hacer valer dichas salvedades cuando ya se ha montado un sistema completo de interceptación y la organización responsable es una agencia secreta de espionaje? Es imposible. Y, de hecho, se han producido casos que demuestran que la FRA ha quebrantado la ley en numerosas ocasiones. Muchos países se limitan a hacerlo fuera de la ley, sin ningún tipo de

cobertura legislativa. De modo que en cierto sentido tenemos suerte si, como en el ejemplo sueco, decidieran, para evitar posibles demandas judiciales, cambiar la ley y legalizarse. Y ése es el caso de la mayoría de los países, se está produciendo una interceptación masiva, y cada vez que surge una propuesta legislativa, ésta es para salvar el culo de aquellos que la están llevando a cabo.

Se trata de una tecnología muy compleja, por ejemplo en el debate suscitado en Australia y el Reino Unido sobre una propuesta de ley para interceptar metadatos, la mayoría de la gente no comprendía el valor de los metadatos, ni siquiera la propia palabra.[4] Interceptar todos lo metadatos significa que tienes que construir un sistema que físicamente intercepte todos los datos y que luego los desestime para quedarse sólo con los metadatos. Pero tal sistema no puede ser fiable. No hay manera de determinar si realmente se están interceptando y almacenando todos los datos sin contar con ingenieros altamente cualificados, con autorización para acceder y revisar meticulosamente lo que está pasando, y tampoco existe voluntad política de garantizar el acceso. El problema es cada vez mayor porque la complejidad y el secretismo son una mezcla tóxica. Oculta tras la complejidad, tras el secreto, se construye la falta de responsabilidad. Es una característica peligrosa por su propio diseño intrínseco.

JÉRÉMIE

No estoy diciendo que el enfoque político funcione. Lo que digo es que ésta es la teoría de cómo funcionaría un sistema democrático y, de hecho, incluso en esta teoría tienes a los servicios secretos, a los que se les permite ir más allá de lo que se considera la norma para los policías e investigadores ordinarios. Así que incluso en el caso de que se regulara el comportamiento de los investigadores ordinarios, siempre habría otra gente capaz de usar esas tecnologías. No obstante, la cuestión principal es si deberíamos regular o no el mero hecho de comprar y poseer dichas tecnologías en contraposición a regular el uso de las mismas.

JULIAN

Te refieres a los kits de interceptación masiva que pueden interceptar la mitad de un país o toda una ciudad.

JÉRÉMIE

Sí. Como las armas nucleares. Uno no puede vender un arma nuclear fácilmente, sin embargo cabe que algunos países quieran construirlas, pero tienen problemas. Cuando hablamos sobre sistemas armamentísticos lo que se regula es la tecnología y no el uso que se hace de ella. Creo que el debate estaría en si estas tecnologías deben o no considerarse tecnologías de guerra.

JACOB

Depende. Cuando son armas —y no hay duda de que los equipos de vigilancia son un arma en países como Siria o Libia— las utilizan en concreto para identificar políticamente a las personas. La compañía francesa Amesys, espió a personas en el Reino Unido utilizando equipos franceses que en Francia eran ilegales, y que vendieron a sabiendas.[5]

ANDY

Y ellos nunca harían algo así ¿no?

JACOB

Bueno, a Amesys la hemos pillado al sacar a la luz sus documentos internos en los llamados *Spy files*.[6] Si hablamos de armas propiamente dichas, hay que tener en cuenta que no es lo mismo que vender un camión a un país. Más bien es como venderle un camión, un mecánico y un equipo que va montado en el camión para identificar selectivamente a las personas y luego dispararlas.

JULIAN

Sería como venderle una flota entera de camiones.

ANDY

Es interesante que la criptografía se regule. Existe el Acuerdo Wassenaar, de ámbito internacional, lo cual

significa que tú no puedes exportar tecnología de encriptación, que sirve para protegernos frente a la tecnología de vigilancia, a aquellos países declarados «malos» o que, por la razón que sea, se consideren «problemáticos». Sin embargo, si lo que tienes son equipos de vigilancia, entonces sí que puedes venderlos internacionalmente. No existen restricciones de exportación sobre este tipo de sistemas. La razón, diría, se debe a que hasta los países democráticos tienen su particular interés en ello, el de controlar. E incluso si estás tratando con países «malos» y les suministras un sistema de vigilancia para hacer «cosas malas/el mal», estarás beneficiándote, pues podrás enterarte de qué escuchan, qué temen, de quiénes son las personas más importantes en la oposición o de los actos políticos que organizan. Y así podrás predecir futuros sucesos, financiar acciones y demás. Éste es el juego sucio que impera entre muchos países, y ésa es la realidad de por qué los sistemas de vigilancia no se regulan.

JULIAN

Me gustaría explorar esta analogía de la vigilancia masiva como arma de destrucción masiva. Fue un hecho constatado por la física que era posible fabricar una bomba atómica, y cuando la bomba atómica se inventó la geopolítica cambió, y también cambió la vida de mucha gente en maneras muy diversas, si bien puede que algunas

fueran positivas, otras fueron totalmente apocalípticas. Un movimiento regulador aplicó controles, y hasta ahora esos controles, salvo en el caso de Japón, nos han salvado de una guerra nuclear. Pero es fácil enterarse de cuándo se utilizan dichas armas y cuándo no.

Con el incremento de la sofisticación y la reducción del coste de la vigilancia masiva de la última década, nos encontramos ahora en una etapa en la que la población humana se duplica cada veinticinco años mientras que la capacidad de vigilancia se duplica cada dieciocho meses. La curva de la vigilancia está dominando la curva de la población. No hay escape directo. Nos encontramos en una etapa en la que con sólo diez millones de dólares podemos comprar una unidad para almacenar permanentemente las interceptaciones masivas de un país de tamaño medio. Así que me pregunto si necesitamos una respuesta equivalente. Esto constituye una gran amenaza real para la democracia y la libertad a nivel mundial que, al igual que la amenaza de la guerra atómica necesitó una respuesta masiva, necesita urgentemente una respuesta que intente controlarlo, ahora que todavía podemos.

ANDY

Yo viví cómo en Libia el movimiento democrático se topó con las estaciones de vigilancia, y las grabaron, proporcionando las pruebas que confirman que compañías

occidentales apoyaban al régimen de Gadafi en la supresión de actos políticos, y cómo después el nuevo gobierno se apropió de estas mismas instalaciones que actualmente han vuelto a funcionar a pleno rendimiento.[7] De modo que, si bien estoy de acuerdo en que sería una buena idea controlar esta tecnología, soy un tanto escéptico respecto a los intereses de los ciudadanos y los intereses de aquellos que detentan el poder. Ni siquiera los llamaría necesariamente gobiernos, porque quien quiera que tenga la capacidad de escuchar todo tipo de llamadas telefónicas, tiene la capacidad de hacer cosas. Esto también incide en la bolsa, económicamente puedes conseguir grandes beneficios si sabes lo que está pasando.

JULIAN

Aquellos países que tienen legislación sobre cuáles deberían ser los objetivos de sus principales agencias de espionaje —agencias como NSA de Estados Unidos, el GCHQ (Cuartel General de las Comunicaciones del gobierno) en Reino Unido, la DSD (la Dirección de Defensa de Señales) de Australia—, todos han modificado sus respectivas leyes para incluir la inteligencia económica. Para ilustrarlo pongamos por caso que Australia y Estados Unidos se estuvieran disputando un contrato de trigo, ambos países espiarían a todas las personas relacionadas con el mismo. Esto viene sucediendo desde hace tiempo, es público y

notorio desde al menos diez años, pero se permite, porque la gente lo sigue haciendo. Empezó con los contratos de armamento, donde compañías como Lockheed Martin, Raytheon y Northrup dedicadas a la venta de armas también participan en la construcción de sistemas de interceptación masiva por tratarse de grupos afines a los círculos de poder. Obtenían favores de sus amigos y basaban las interceptaciones de los contratos armamentísticos en criterios de seguridad nacional. Sin embargo ahora esto se aplica a todo aquello que pueda beneficiar económicamente a un país, que es casi todo.

JACOB

Una buena analogía planteada por algunos de los participantes en el Congreso de Comunicación del Caos, en diciembre de 2011, fue la de equiparar la tecnología de vigilancia, especialmente la tecnología de vigilancia táctica pero también la tecnología de vigilancia estratégica, a las minas antipersona.[8] Creo que es una idea muy potente. El mero hecho de que sea posible no significa que sea inevitable que acabemos tomando este camino, y tampoco significa que todos tengamos que llegar al punto de que todo el mundo sea monitorizado.

Sin embargo, existen incentivos económicos en nuestra contra. Por ejemplo, alguien me contó que el sistema telefónico noruego solía operar con un contador que,

dependiendo de lo lejos que llamaras, funcionaba a mayor o menor velocidad. No obstante, era ilegal que la compañía telefónica noruega almacenara o conservara un registro de los metadatos (como el número telefónico marcado) concernientes a la llamada efectuada, y ello se debía principalmente a cuestiones de privacidad relacionadas con la segunda guerra mundial. Por tanto es posible construir esa misma tecnología de modo tal que respete la intimidad sin perder de vista el enfoque de mercado, lo cual seguiría generando un beneficio económico. Sin embargo, con lo que tenemos todas las de perder es con las tecnologías GSM (móviles). Por el momento el modo en que están diseñados estos sistemas, no sólo en términos de facturación sino también en cuanto a su arquitectura, no permiten la privacidad de ubicación, carecen de privacidad de contenidos.

JULIAN

El teléfono móvil es un dispositivo de rastreo que también permite hacer llamadas.

JACOB

Exacto. Si, por ejemplo, hablamos de que todos en el tercer mundo están siendo espiados, ¿qué quiere decir esto realmente? Significa que sus sistemas de telefonía, que son su vínculo con el resto del mundo, se convierten en

dispositivos de espionaje cuando alguien decide utilizar los datos almacenados para tal fin.

ANDY

Yo he visto a países africanos recibir la infraestructura de internet al completo, incluido el cable de fibra óptica y los conmutadores centrales, como regalo de los chinos.

JACOB

¿Como regalo de ZTE o de alguna compañía parecida? [9]

ANDY

Sí, y por supuesto los chinos tienen su interés en los datos, de modo que no necesitan cobrarse la instalación en dinero, se lo cobran en datos, la nueva moneda.

Espionaje del sector privado

JÉRÉMIE

La vigilancia financiada por los Estados es un asunto capital que desafía a la estructura intrínseca de todas las democracias y al modo en que éstas funcionan, pero también existe la vigilancia privada que potencialmente puede derivar en la recopilación masiva de datos. Sólo hay que fijarse en Google. Si eres un usuario estándar de Google, el buscador sabe con quién te comunicas, a quién conoces, a quién buscas, tu posible orientación sexual y tus creencias religiosas y filosóficas.

ANDY

Sabe más de ti que tú mismo.

JÉRÉMIE

Más que tu madre, seguro, y puede que incluso más

que tú mismo. Google sabe cuándo estás conectado y cuándo no.

ANDY

¿Acaso sabes lo que buscaste hace dos años, tres días y cuatro horas? No lo sabes; Google sí.

JÉRÉMIE

De hecho, yo trato de no volver a usar Google por estas mismas razones.

JACOB

Es como el movimiento *Kill your television* (mata tu televisor) del siglo XXI.[1] Protesta efectiva, salvo que el efecto de red evita que tu protesta funcione.[2] Mata tu televisor, tío.

JÉRÉMIE

Bueno, no es una protesta, diría que es más bien mi particular modo de ver las cosas.

ANDY

Yo vi en su día esos preciosos documentales de gente tirando televisores por la ventana desde edificios de tres plantas.

JÉRÉMIE

No es sólo la vigilancia financiada por los Estados. Es la cuestión de la privacidad, la forma en que la información está siendo manejada por terceros y el conocimiento que la gente tiene sobre lo que se está haciendo con dicha información. Yo no uso Facebook, así que no sé mucho sobre esta red social. Pero ahora con Facebook ves el comportamiento de usuarios felices de revelar cualquier tipo de información personal y, ¿se puede culpar a la gente por no saber dónde está el límite entre la privacidad y la publicidad? Hace años, antes de que irrumpieran las tecnologías digitales, las personas que tenían una vida pública pertenecían al mundo del espectáculo, a la política o al periodismo, y ahora cualquiera tiene el potencial para acceder a la vida pública a golpe de clic en el botón publicar. «Publicar» significa hacer algo público, significa permitir el acceso a esta información al resto del mundo —y, por supuesto, cuando ves a adolescentes enviando fotos de sí mismos borrachos o en cualquier estado parecido, puede que no tengan la perspectiva de lo que realmente significa ponerlas a disposición del «resto del mundo», y, potencialmente, durante un larguísimo periodo de tiempo. Facebook hace negocio difuminando esta línea entre la privacidad, los amigos y la publicidad. E incluso está almacenando información en principio destinada únicamente a tus amigos y seres queridos. Así que independientemente del grado de publicidad que quieras dar a tu información, cuando haces

clic en el botón publicar de Facebook, antes se la das a Facebook y luego ellos permiten el acceso a los otros usuarios de tu círculo de Facebook.

JULIAN

Incluso la línea entre el gobierno y la empresa privada se ha disipado. Basta con observar la expansión que ha experimentado el sector de contratistas militares en Occidente durante la última década, la Agencia de Seguridad Nacional estadounidense, la mayor agencia de espionaje del mundo, tenía sobre el papel diez contratistas principales con los que trabajaba. Hace dos años, tenía más de mil. De modo que se ha desdibujado la frontera que delimita lo que es el gobierno y lo que es el sector privado.

JÉRÉMIE

Y se puede argüir que las agencias de espionaje estadounidenses tienen acceso a toda la información almacenada por Google.

JULIAN

Y, de hecho, lo hacen.

JÉRÉMIE

Y a todos los datos de Facebook, así que, en cierto sentido, Facebook y Google serían extensiones de estas

agencias.

JULIAN

¿Tienes una citación de Google, Jake? ¿Se remitió una citación a Google requiriéndole información relacionada con tu cuenta de Google? De WikiLeaks sí, remitieron citaciones al registro de nuestro nombre de dominio con base en California, dynadot, donde se efectuó el registro de Wikileaks.org. Eran citaciones relacionadas con la investigación que sobre WikiLeaks llevaba a cabo un gran jurado secreto, y en las que se le pedían registros financieros, registros de acceso a cuentas, etcétera; información que dynadot les entregó.[3]

JACOB

El diario *The Wall Street Journal* reveló que Twitter, Google y Sonic.net, tres servicios que uso o he usado en el pasado, recibieron un aviso 2703(d), que es la forma inusual de citación secreta.[4]

JULIAN

¿Amparándose en la Ley PATRIOTA?

JACOB

No. Se trata de la Ley de Comunicaciones Almacenadas. El diario *The Wall Street Journal* revela que cada uno de

estos servicios afirma que el gobierno quería los metadatos, y que éste aseveró estar en su derecho de reclamarlos sin mandamiento judicial. Actualmente hay una causa abierta que estudia el derecho del gobierno a mantener sus tácticas en secreto, no sólo de cara al público sino también frente a las instancias judiciales. Me enteré de esto como el resto del mundo, cuando lo leí en el diario.

JULIAN

Así que Google siguió el juego al gobierno estadounidense en la investigación de su gran jurado sobre WikiLeaks cuando éste le requirió los registros que tenía de ti, y no a través de una citación judicial convencional, sino sirviéndose de este tipo concreto de pseudocitación de inteligencia. Sin embargo la noticia surgió con anterioridad, en el año 2011, cuando al ser objeto de una serie de citaciones por parte del gran jurado, Twitter presentó una demanda judicial en la que solicitaba el levantamiento de secreto para poder informar a los interesados de la intervención de sus cuentas. Yo no tengo una cuenta de Twitter, así que no recibí nada, pero mi nombre y el de Bradley Manning aparecían en todas las citaciones como parte de la información solicitada. Jake, tú tenías una cuenta de Twitter, así que Twitter recibió la citación de marras para investigarte. Google también recibió la suya, sin embargo no presentó ninguna demanda para hacerla pública.[5]

JACOB

Eso parece. Es lo que leí en *The Wall Street Journal*. Puede que ni siquiera se me permita mencionarlo, salvo aquello publicado en *The Wall Street Journal*.

JULIAN

¿Se debe a que estas «órdenes» tienen también un componente secreto? Eso se ha declarado inconstitucional ¿no?

JACOB

Puede que no. En el caso de Twitter es de dominio público que el tribunal desestimó el recurso en el que solicitábamos la suspensión de la ejecución de la «orden» alegando que la revelación de esta información al gobierno causaría un daño irreparable, pues una vez conseguida esta información no se olvida. Ellos dijeron: «Sí, bueno, desestimamos el recurso presentado, Twitter debe revelar esta información». Estamos en proceso de apelación, concretamente en lo que respecta al secreto de los expedientes —y no puedo hablar de ello— pero, a día de hoy, el tribunal ha declarado que en internet no cabe la expectativa de privacidad cuando tú voluntariamente revelas información a terceros, y, dicho sea de paso, en internet todo el mundo es un tercero.

JULIAN

Incluso en el caso de que organizaciones como Facebook o Twitter digan que mantendrán la privacidad de la información.

JACOB

No te quepa la menor duda. Por eso se están desdibujando los límites entre el Estado y la empresa privada. Posiblemente este sea el punto más importante a tener en cuenta, que la Agencia de Seguridad Nacional y Google se han asociado en el asunto de la ciberseguridad por razones patrias de defensa nacional.

ANDY

O lo que quiera que signifique ciberseguridad en este contexto. Es un término amplísimo.

JACOB

Tratan de excluir todo de la Ley de Libertad de Información y mantenerlo en secreto. Y por otro lado el gobierno estadounidense se declara competente para enviar una citación administrativa, de menor rango que una simple orden de registro, en la que se impide a un tercero informarte de que te están investigando, y tú no tienes ningún derecho porque es el tercero en cuestión el que está directamente implicado, y el tercero receptor de la citación tampoco cuenta con asideros constitucionales para proteger tus

datos.

JULIAN

Ya sea el tercero, Twitter, Facebook o tu ISP (Proveedor de Servicios de Internet).

JACOB

O cualquiera. Ellos decían que la banca privada y las llamadas telefónicas se regían por el mapeo asociado uno-a-uno. Sin embargo, revelas voluntariamente cualquier número a la compañía telefónica en cuanto lo marcas. Sabías eso ¿no? En cuanto descuelgas el teléfono es evidente que estás diciendo: «No tengo ninguna expectativa de privacidad» al marcar el número. Existe incluso una conexión menos explícita a la máquina. La gente no entiende cómo funciona internet —tampoco entienden las redes telefónicas— pero los tribunales vienen dictaminando constantemente que esto es así, y, hasta la fecha en nuestra causa de Twitter, el tribunal se ha pronunciado en este mismo sentido.[6]

Es una completa locura imaginar que cedemos toda nuestra información personal a estas compañías, y que luego estas compañías se han convertido básicamente en una policía secreta privatizada. Y, en el caso de Facebook, incluso hemos democratizado la vigilancia. En lugar de untar a la gente como hacía la Stasi en Alemania del Este, les recompensamos como «cultura», ahora el premio es

acostarse unos con otros. La gente habla de sus amigos y luego: «Eh, mengano y fulana salen juntos»; «¡Vaya! fulano y mengana han roto»; «¡Eh! ¡Ya sé a quién puedo llamar ahora!».

ANDY

Hubo gente capaz de presionar a Facebook para que distribuyera toda la información que esta red social almacenaba sobre ellos amparándose en la Ley Europea de Protección de Datos, la cantidad más pequeña de información almacenada era de 350 megas, y la más grande rondaba los 800 megas.[7] Lo interesante es que la estructura de la base de datos de Facebook ha salido a la luz gracias a este acto. Cada vez que introducimos nuestra dirección IP, todo se almacena, cada vez que hacemos clic en internet, todas y cada una de las veces, también el número de veces que visitamos una página, lo cual les permite deducir si es o no de nuestro gusto y todo tipo de información adicional. Sin embargo, esto también reveló que el identificador clave de la estructura de la base de datos era la palabra *target* (objetivo). No llamaban a esta gente ««suscriptores» o «usuarios» o cualquier otra cosa parecida, sino «*targets*», lo cual nos induce a pensar: «Vale, es un término de marketing».

JULIAN

Pero era un concepto de uso interno, privado.

ANDY

Sí, pero también podría ser un *target* (objetivo, blanco) en sentido militar, podría ser un objetivo de los servicios inteligencia. De modo que todo depende de las circunstancias en que esta información se utilice.

JULIAN

De acuerdo. Eso es lo escalofriante del tema.

ANDY

Yo creo que eso es de gran ayuda. Solíamos decir que con Facebook el usuario no es realmente el cliente. El usuario de Facebook es en realidad el producto, y los verdaderos consumidores son las empresas de publicidad. Ésta es la manera menos paranoica, la explicación más inofensiva de lo que está pasando aquí.

Sin embargo el problema es que difícilmente podemos culpar a una empresa por cumplir las leyes de un país. Se considera normal, y lo que es un delito es que las empresas no cumplan las leyes de un país. De modo que cuesta trabajo decir: «Eh, están cumpliendo la ley». ¿Qué tipo de acusación es ésa?

JACOB

No, hay un punto en el que no estoy de acuerdo contigo. Si construyeras un sistema que registra todo sobre una persona sabiendo que vives en un país con leyes que obligarán al gobierno a ceder dicha información, entonces tal vez no deberías construir ese tipo de sistema. Y aquí radica la diferencia entre el enfoque de privacidad-por-política y el de privacidad-por-diseño a la hora de crear sistemas seguros. Cuando intentas identificar a las personas como posibles objetivos/blancos y sabes que vives en un país que, de forma explícita, se dedica a identificar a las personas como objetivos, entonces si Facebook pusiera sus servidores en la Libia de Gadafi o en la Siria de Assad, eso sería algo a todas luces absolutamente negligente. Con todo, ninguna de las Cartas de Seguridad Nacional que salieron a la luz hace, creo, uno o dos años, respondía a cuestiones de terrorismo. Cerca de 250.000 de estas cartas se utilizaron con fines distintos al de erradicar el terrorismo.[8] De modo que sabiendo que ésa es la realidad, estas compañías tienen una importante responsabilidad ética derivada del hecho de construir estos sistemas y de haber elegido la opción económicamente ventajosa de vender a sus usuarios. Y esto ni siquiera es una cuestión técnica. No tiene nada que ver con la tecnología, tiene que ver con la economía. Ellos han decidido que es más importante colaborar con el Estado y vender a sus usuarios violando su privacidad y formando parte del sistema de control —para ser compensados por

formar parte de la cultura de la vigilancia, de la cultura del control— que combatirlo, así que se han vuelto parte del mismo. Son cómplices y responsables.

ANDY

La responsabilidad ética no es precisamente un argumento de venta muy en boga en estos tiempos ¿cierto?

Combatir la vigilancia total con las leyes de la física

JÉRÉMIE

Una pregunta que puede surgir a estas alturas sería: ¿Cuál es la solución tanto para el usuario individual como para la sociedad en general? Hay soluciones técnicas: servicios descentralizados, que todo el mundo aloje sus propios datos, datos cifrados, que todo el mundo confíe en proveedores de su entorno que les ayuden con los servicios de información encriptada, y demás. Y luego están las opciones de política (corporativa y estatal) que hemos debatido. No tengo claro si en este momento podemos responder a la pregunta, ni si alguno de los dos enfoques planteados es mejor que el otro. Creo que tenemos que desarrollar ambos enfoques en paralelo. Necesitamos tener software libre que todo el mundo pueda entender, que todo el mundo pueda modificar y que todo el mundo pueda escudriñar para saber con certeza lo que está haciendo. Creo

que el software libre es la base para conseguir una sociedad virtual libre, para tener el potencial que siempre nos permita controlar a la máquina y no dejar que la máquina nos controle a nosotros. Necesitamos contar con una criptografía sólida para estar seguros de que cuando queramos leer nuestra información en privado, nadie más pueda hacerlo. Necesitamos herramientas de comunicación como Tor o como el Criptophone (teléfono móvil cifrado), para poder comunicarte sólo con aquellos que quieras comunicarte. Sin embargo el poder del Estado y el poder de ciertas empresas siempre puede superar al poder de unos cuantos *geeks* como nosotros y a la capacidad que tenemos para construir y distribuir esas tecnologías. También necesitaríamos, al construir esas tecnologías, leyes y herramientas que estén en manos de los ciudadanos para que ellos puedan controlar lo que se está haciendo con la tecnología —aunque no sea siempre en tiempo real— y sancionar a aquellos que la utilicen de manera poco ética, o violando la privacidad de los ciudadanos.

JULIAN

Quiero comentar lo que yo personalmente veo como una diferencia entre la perspectiva criptopunk estadounidense y la perspectiva europea. La Segunda Enmienda de Estados Unidos contempla el derecho a portar armas. Hace relativamente poco estuve viendo unas

secuencias que un amigo rodó en Estados Unidos sobre este tema, y justo encima de la puerta de una tienda de armas de fuego había un cartel que rezaba: «Democracia, cargada y con el seguro puesto». De ese modo os aseguráis de que no tenéis regímenes totalitarios —las personas van armadas y si las cabreas más de la cuenta, se limitan a sacar sus armas y a retomar el control por la fuerza. Si dicho razonamiento sigue o no teniendo validez es una cuestión interesante dada la evolución que las armas han experimentado durante los últimos treinta años. Amparándonos en esta declaración podríamos decir que la codificación, el suministro de códigos secretos que el gobierno no podía descifrar, era en sí misma una munición. Nosotros luchamos en esta gran guerra de la década de los noventa para que todo el mundo pudiera disponer de la criptografía, y en gran medida la ganamos.[1]

JACOB

En Occidente.

JULIAN

Ganamos en gran parte de Occidente y la criptografía está en todos los navegadores, aunque puede que en la actualidad haya sido «interceptada a través de puertas traseras» (*backdoored*) y subvertida de múltiples formas.[2] La idea es que no podemos confiar en un gobierno que

implementa las políticas que dice que está implementando, y por eso debemos facilitar las herramientas subyacentes, herramientas criptográficas que nosotros controlamos, como un elemento de fuerza con codificaciones lo suficientemente buenas para que ningún gobierno, aunque lo intente por todos los medios, pueda inmiscuirse en nuestras comunicaciones.

JACOB

La fuerza de casi todas las autoridades modernas se deriva de la violencia y de la amenaza de violencia. Debemos asumir que con la criptografía ningún tipo de violencia resolverá nunca un problema matemático.

JULIAN

Exacto.

JACOB

Ésa es la clave. Esto no quiere decir que no te puedan torturar, no significa que no puedan pincharte el teléfono o instalar micrófonos en tu casa, lo que significa es que si se encuentran con un mensaje cifrado, al margen de la fuerza de la autoridad que les respalda, ellos no pueden resolver ese problema matemático. Sin embargo, esto es algo que no resulta en absoluto evidente para el común de los mortales y tenemos que hacérselo entender. Si todos pudiéramos

resolver todos esos problemas matemáticos sería otra historia y, por supuesto, el gobierno también podría hacerlo.

JULIAN

El caso es que es parte de nuestra realidad, como lo es el hecho de que se pueden fabricar bombas atómicas, que podemos crear problemas matemáticos que ni siquiera las mayores potencias son capaces de descifrar. Creo que eso caló tremendamente en los libertarios californianos y otros grupos que creían en este tipo de idea de «democracia cargada y con el seguro puesto», porque aquí planteábamos hacerlo por la vía intelectual: la de un par de individuos con criptografía enfrentándose al poderío de la mayor potencia del mundo.

Así que el universo tiene una propiedad que está del lado de la privacidad, porque existen algunos algoritmos criptográficos que ningún gobierno podrá romper jamás. También hay otros que sabemos que son extremadamente difíciles de descifrar incluso para la Agencia de Seguridad Nacional. Lo sabemos porque ellos fueron quienes recomendaron su uso a los contratistas militares estadounidenses para proteger las comunicaciones de alto secreto del Ejército, y si hubiera algún tipo de puerta trasera (*backdoor*), más temprano que tarde los rusos o los chinos la encontrarían, con serias consecuencias para quien quiera que tomara la decisión de recomendar un código inseguro.

Así que los códigos ahora son bastante buenos, nosotros tenemos gran confianza en ellos. Desafortunadamente en lo que no podemos confiar es en las máquinas que operan con ellos, y ese es el problema. Pero eso no conduce a la interceptación masiva; nos lleva a la identificación de ordenadores que pertenecen a personas muy concretas. A menos que seas un experto en seguridad es realmente complicado asegurar un ordenador. Sin embargo, la criptografía puede resolver este problema de interceptación masiva, pues es la interceptación masiva y no la identificación de objetivos individuales lo que constituye una verdadera amenaza para la civilización global.

No obstante, soy consciente de que nos enfrentamos a fuerzas económicas y políticas tremendamente potentes, y el resultado más probable es que la eficiencia natural de las tecnologías de vigilancia, comparada con el número de seres humanos, nos conduzca irrevocablemente a una sociedad totalitaria de vigilancia global —y por totalitaria entiendo vigilancia total—, en la que tan sólo queden unos cuantos seres humanos capaces de vivir en libertad: aquellos que entiendan cómo usar esta criptografía para defenderse de esta vigilancia total y absoluta, y aquellos que vivan completamente desconectados, *neoluditas* que se internan en sus cuevas, o miembros de tribus tradicionales que carecen de las eficiencias de la economía moderna y cuya capacidad de acción es prácticamente nula. Ellos mismos

reniegan de su influencia al elegir ese tipo de vida. Ocurre lo mismo con los teléfonos móviles; siempre puedes elegir no tener uno, pero eso significa que limitas tu capacidad de influencia. No es un camino a seguir.

JÉRÉMIE

Si lo planteamos desde una perspectiva de mercado, estoy convencido de que existe un mercado para la privacidad que está sin explorar, así que puede que haya algún acicate económico para que las empresas desarrollen herramientas que permitan a los usuarios ser capaces de controlar individualmente su información y sus comunicaciones. Tal vez sea ésta una de las formas de resolver el problema. No sé si con esto basta para que funcione, pero es una posibilidad, y tal vez todavía no hayamos caído en la cuenta.

JULIAN

La criptografía estará en todas partes. Está siendo utilizada por las principales organizaciones del mundo, que gradualmente entretejen una red de ciudades-Estado interconectadas. Si pensáis en las vías de comunicación de internet —rápidos flujos de dinero transnacional, organizaciones transnacionales, interconexiones entre subpartes de organizaciones—, se producen a través de canales de comunicación poco fiables. Es como un

organismo sin piel. Cuentan con organizaciones y Estados solapándose unos con otros —cada red de influencia mundial compitiendo por sacar el máximo beneficio— y sus flujos de información están expuestos a oportunistas, competidores estatales y demás. De modo que se están construyendo nuevas redes por encima de internet, redes virtuales privadas cuya privacidad proviene de la criptografía. Esa es una de las bases industriales de poder que está frenando la prohibición de la criptografía.

Si echas un vistazo a la Blackberry por ejemplo, lleva integrado un sistema de encriptación para usar dentro de la red Blackberry. Research In Motion, la empresa canadiense que lo comercializa, puede desencriptar el tráfico de los usuarios regulares y cuenta como mínimo con centros de datos en Canadá y Reino Unido, de modo que una alianza anglo-americana de inteligencia puede interceptar todas las comunicaciones mundiales de Blackberry a Blackberry. Sin embargo, las grandes compañías se valen de formas más seguras. Los gobiernos occidentales estaban de acuerdo hasta que la criptografía pasó de la empresa a los individuos, y fue entonces cuando pudimos ver las mismas reacciones hostiles a nivel político que las que observamos en el Egipto de Mubarak.[3]

Creo que la única defensa efectiva ante la inminente distopía de vigilancia es aquella que te permita dar los pasos necesarios a nivel individual para salvaguardar tu

privacidad, pues no hay incentivo alguno para la autocontención por parte de aquellos que tienen la capacidad de interceptarlo todo. Para ilustrarlo con una analogía histórica pensemos en cómo la gente aprendió que debía lavarse las manos. Para ello hizo falta establecer y popularizar una teoría microbiana de la enfermedad, así como difundir la paranoia sobre su propagación a través de microbios invisibles alojados en las manos, algo que no podemos ver, como tampoco podemos ver la interceptación masiva. Una vez la gente hubo entendido el problema, los fabricantes de jabón lanzaron productos que la gente consumía para mitigar el miedo. Por tanto es necesario infundir miedo en la gente para que entiendan el problema y se genere así la demanda suficiente que permita resolverlo.

También hay un problema en el lado opuesto de la ecuación, el problema radica en que los programas que afirman ser seguros, que afirman tener criptografía integrada, son a menudo fraudes, porque la criptografía es compleja, y el fraude puede esconderse en la complejidad.[4]

Así que la gente tendrá que pensar en ello. La única pregunta es: de cuál de las dos maneras pensará sobre ello. Pueden pensar: «Debo tener cuidado con lo que digo, necesito adecuarme a lo que hay», todo el tiempo, en cada una de sus interacciones. O bien pueden pensar: «Necesito dominar ciertos elementos de esta tecnología e instalar cosas que me protejan a fin de poder expresar mis

pensamientos, y poder comunicarme libremente con mis amigos y aquellos que me importan». Si la gente no adopta la segunda opción, entonces viviremos en una corrección política universal, porque incluso cuando las personas se comuniquen con sus amigos más íntimos se autocensurarán, y, consiguientemente, se estarán autoexcluyendo del mundo como actores políticos.

Internet y la política

JÉRÉMIE

Es interesante ver el poder de los hackers —«hackers» en el sentido primigenio de la palabra, no en el que le equipara a un criminal—. Un hacker es un apasionado de la tecnología, alguien a quien le gusta entender cómo funciona la tecnología, no para quedar atrapado en ella sino para mejorar su funcionamiento. Supongo que cuando vosotros teníais cinco o seis años cogisteis un destornillador e intentasteis abrir dispositivos para entender cómo eran por dentro. Esto es exactamente lo que hace un hacker, y los hackers construyeron internet por muchas razones, también porque era divertido, y la desarrollaron y se la dieron al resto del mundo. Compañías como Google y Facebook vieron la oportunidad de construir a posteriori modelos de negocio basados en la captura de datos personales de los usuarios. No obstante, nosotros todavía vemos una forma de poder en

manos de los hackers. Mi principal interés en la actualidad es que veamos a estos hackers ganando poder, incluso en la arena política. En Estados Unidos se aprobó la SOPA (Stop Online Piracy Act /Ley de cese a la piratería en línea) y el PIPA (Protect IP Act/Proyecto de Ley de protección de propiedad intelectual), una violenta ley de derechos de autor que básicamente otorga a Hollywood el poder para ordenar a cualquier empresa virtual que restrinja el acceso y censure internet.[1]

JULIAN

Y bloqueos bancarios como el que está sufriendo WikiLeaks.[2]

JÉRÉMIE

Exactamente. Lo que los bancos hicieron a WikiLeaks se estaba convirtiendo en el método estándar para luchar contra los malvados piratas de derechos de autor que mataban a Hollywood y esas cosas. Y nosotros presenciamos este tremendo clamor de la sociedad civil en internet, y no sólo en Estados Unidos. No habría funcionado de haber sido sólo los ciudadanos estadounidenses quienes se levantaran contra la SOPA y el PIPA. Participó gente de todo el mundo, y los hackers estaban en el corazón mismo de la protesta proporcionando herramientas al resto y ayudándoles a participar en el debate público.

JULIAN

Ayudando a hacer la campaña.

JÉRÉMIE

¿No era Tumblr o algún sitio web del estilo donde la página de inicio te permitía introducir tu número de teléfono y te devolvía la llamada para ponerte en contacto con el Congreso? Y tú te limitabas a responder a quienquiera que estuviera al otro lado diciendo: «Vale, esto es una gilipollez».

JACOB

Internet se utilizaba en defensa de sí misma.

JÉRÉMIE

Creo que nosotros los hackers tenemos una responsabilidad con respecto a las herramientas que construimos y cedemos al resto del mundo, y puede que estemos presenciando el principio de lo eficazmente que esta responsabilidad puede activarse cuando la utilizamos de forma colectiva. Hoy en Estados Unidos se está debatiendo el ACTA (Acuerdo Comercial de la Lucha contra la Falsificación), un tratado de carácter internacional que constituye el marco ideal para la ley SOPA y el proyecto de ley PIPA.[3] Hace pocos días estuve en el Parlamento Europeo donde nosotros, como individuos, barbudos y

apestosos individuos, estuvimos dictando condiciones a una comisión parlamentaria. En el Parlamento Europeo les mostramos artículos del reglamento que aparentemente veían por primera vez y les dijimos cómo actuar, y se produjo esta votación que ganamos con una diferencia de 21 a 5 votos que dejó al ponente británico relegado a un segundo plano. Fue una pequeñísima parte de un pequeño punto de procedimiento para acabar con el Acuerdo Comercial de la Lucha contra la Falsificación, este monstruoso acuerdo global que ha sido diseñado a nuestras espaldas para sortear la mismísima democracia. Pero nosotros como ciudadanos somos capaces de matar a ese monstruo —fácilmente, con las herramientas de internet, listas de correo, los *wikis*, los foros de chateo IRC, etcétera—, y tal vez estemos presenciando la llegada de la mayoría de edad de internet, los años de adolescencia de internet y la manera en que se puede utilizar por la sociedad en su conjunto para lograr que las cosas cambien. Creo que es clave que nosotros los hackers estemos aquí, con nuestro conocimiento técnico, para guiar a las personas y para decirles: «Debes usar esta tecnología porque, a diferencia de Facebook o Google, te permite controlar tu privacidad». Y que ambas partes nos articulemos bien, o podamos articularnos bien. Al menos nos queda margen para un poco de optimismo.

JULIAN

Jake, en esta radicalización política de la juventud de internet, concretamente durante estos dos años has viajado por todo el mundo hablando de Tor, hablando con personas que buscan el anonimato, que quieren disfrutar de la privacidad y evitar el control que ejercen sus respectivos gobiernos, y has debido observar este fenómeno en muchos países diferentes. ¿Es algo significativo?

JACOB

Claro. Creo que es totalmente significativo. El ejemplo canónico que se me ocurre a bote pronto es Túnez. Fui a Túnez tras la caída del régimen de Ben Ali y hablamos sobre Tor en una clase de ciencias de la computación a la que asistieron estudiantes altamente especializados de la universidad, allí una chica levantó la mano y dijo: «Pero ¿qué pasa con los malos?». Y soltó a la carrera la retahíla de Los cuatro jinetes del Info-Apocalipsis —blanqueo de dinero, drogas, terrorismo y pornografía infantil—. «¿Qué pasa con los malos?» Estas cuatro cosas siempre salen a colación y su espectro se utiliza para echar por tierra cualquier tipo de tecnología tendente a preservar la privacidad, porque está claro que tenemos que acabar con esos cuatro grupos. Así que pregunté a la clase: «¿Quién de aquí ha visto alguna vez la página web Ammar 404?». Es la web de censura desarrollada por el régimen de Ben Ali antes y durante la revolución para impedir el acceso a internet. El profesor y

todos los estudiantes de la clase, salvo la persona que planteó la pregunta, levantaron la mano. Y yo miré a la chica que me había preguntado y le dije: «Mira a tu alrededor. Son todos tus compañeros de clase. ¿Crees realmente que merece la pena oprimir a todas las personas de esta clase para luchar contra esas cosas?». Y ella respondió: «La verdad es que yo también levanto mi mano».

El debate fue más extenso, pero básicamente las personas que lo contextualizaron en su entorno se dieron cuenta de que el verdadero reto era éste. Eso cambia las cosas radicalmente. Y esto ocurre en todo el mundo, todo el tiempo. El problema es que normalmente ocurre tarde, la gente se da cuenta a posteriori de que podía haber usado la tecnología. Ven a posteriori que: «Oh, sí, resulta que no son los malos porque, de hecho, el malo soy yo si expreso mi opinión a otra persona sobre algo que quienes detentan el poder no quieren que exprese». Y te das cuenta de que la gente está abriendo los ojos.

Pero no es cierto que esto se limite a los dos últimos años. Siento hacerte esto, Julian, pero tú eres parte de la radicalización de mi generación. Digamos que yo pertenecería a la tercera generación del movimiento criptopunk si lo planteo de este modo. El trabajo que tú y Ralf Weinmann hicisteis con el sistema de archivos Rubberhose fue parte de lo que me inspiró a dedicarme a los sistemas criptográficos. Diseñé el sistema de cifrado de

archivos que lleva el nombre de M.A.I.D, en respuesta a cosas como los poderes reguladores e investigadores del Reino Unido —donde básicamente el Estado ha decidido que una reglamentación negativa es la solución a la criptografía— donde el Estado puede quedarse con tu contraseña sin ningún problema.[4] Por supuesto, en el caso de Julian era distinto, crearon su sistema porque los regímenes opresivos torturaban a la gente para averiguar una clave de acceso, de modo que tenías que poder facilitar distintas claves para someterte a sus torturas. Mi sistema de cifrado M.A.I.D. fue diseñado para un sistema legal en el que, si bien el acusado tiene el derecho a permanecer en silencio, también puede demostrar, si le obligan, que está diciendo la verdad sin violar la confidencialidad. Al ver el trabajo de Julian me di cuenta de que la tecnología se podía usar para conferir a la gente de a pie el poder de cambiar el mundo. Remontándome en el tiempo, remontándome a los tiempos de la vieja lista de correo Criptopunk con Tim May, uno de los miembros fundadores del movimiento, y leyendo las antiguas entradas de Julian en la lista Criptopunk, estoy convencido de que eso fue el génesis de toda una generación que pronto adoptaría posturas más radicales, porque la gente empezó a darse cuenta de que podía acabar con la atomización que padecía, de que podía dedicar algo de tiempo a escribir un tipo de software que empoderara a millones de personas.[5]

Sin embargo existen algunas consecuencias inesperadas en el desarrollo de los acontecimientos, porque la gente que creó Google no tenía en mente crear Google, crear la maquinaria de vigilancia más grande jamás inventada. Sin embargo eso ha sido lo que, de hecho, se ha creado, y en cuanto la gente empiece a darse cuenta, empezará a enviar las mentadas cartas de seguridad nacional, ¿cierto?

JÉRÉMIE

Yo veo tres puntos entrelazados. No digo que deban plantearse por separado, pero uno de ellos es sin duda el de los regímenes autoritarios y el poder que los regímenes autoritarios detentan en la era de las tecnologías digitales. En el caso del régimen de Ben Ali —ocurre también en otros muchos regímenes de nuestros días—, unos cuantos deciden lo que la gente puede saber y con quién puede comunicarse. Esto supone un tremendo poder al que deberíamos oponernos, e internet —una internet libre— es una herramienta para enfrentarnos a él. Otro punto es el de construir herramientas y una mejor tecnología, tecnología que trate de sortear problemas como la censura, pero sobre todo construir herramientas que conformen la infraestructura que nos ayude a derrocar a los dictadores. Y luego está el tercer asunto, el discurso político de Los cuatro jinetes del Info-Apocalipsis que mencionabas, los pretextos que los

políticos utilizan a diario en los medios de comunicación: «¿Vamos todos a morir a causa del terrorismo? Por tanto necesitamos una Ley Patriota»; «Los consumidores de pornografía infantil están por todas partes»; «Hay pedo-nazis por toda la red, por eso necesitamos la censura».

JACOB

¿Pedo-nazis?

JÉRÉMIE

Pedo-nazis, sí —pedo-nazi.com ya está registrada—. «Los artistas van a morir y el cine dejará de existir, por tanto tenemos que dar a Hollywood el poder para censurar internet», y todo ese rollo. Creo que aquí de nuevo internet es una herramienta, un antídoto contra la narración política. La narración política se basa en la emotividad y en el corto espacio de tiempo de que dispone en los medios de comunicación —la información aparece y desaparece en cuestión de veinticuatro horas y luego se sustituye por nueva información. Con internet tengo la impresión de que estamos construyendo lo que yo llamo el tiempo de internet. Como la gran internet nunca olvida, podemos recopilar expedientes durante años, día tras día, y podemos elaborar, podemos analizar. Esto es lo que hemos estado haciendo durante los tres últimos años con el acuerdo ACTA. Una vez más, WikiLeaks ha sido una inspiración para nosotros

porque la primera versión del ACTA que se filtró, acabó en WikiLeaks en el año 2008.[6]

JULIAN

Sí, nosotros la difundimos.

JÉRÉMIE

Y nosotros filtramos otras dos versiones más. Se han hecho cinco versiones del texto durante los tres años que pudimos estudiarlo y, párrafo a párrafo, línea a línea, nos dedicamos a explicar que tal cosa origina aquella, que ésta es la industria pidiendo esto o lo de más allá, involucrando a expertos legales y a especialistas en tecnología para crear una versión de la narración política que era diferente de la oficial: «¡Oh! Necesitamos el ACTA para salvaguardar nuestra cultura y a nuestros niños de los medicamentos falsos», y ese tipo de cosas. Y así trazamos nuestra propia línea política con el tiempo de internet, con análisis precisos, con trabajo duro, poniendo a gente en contacto para que participara en el proyecto.

JULIAN

Eso es cierto, y creo que esa visión del ACTA se ha ganado al público.

JÉRÉMIE

Hasta el momento está respondiendo bien.

JULIAN

Creo que ésa será la visión histórica, pero entre bastidores el llamado Acuerdo Comercial de la Lucha contra la Falsificación, que impulsó la industria estadounidense de derechos de autor, ha sido reiteradamente utilizado en cantidad de tratados bilaterales con el fin de crear un nuevo régimen internacional sobre lo que es legal y lo que no, en lo concerniente a la publicidad, identificando los mecanismos existentes para evitar que la gente publique ciertas informaciones. Este acuerdo tipifica en suma una versión más dura de la DMCA (*Digital Millenium Copyright Act*/ ley estadounidense de derechos de autor digitales del milenio), bajo cuyos auspicios si enviabas una carta a alguien exigiendo que eliminara algo de internet, tenía obligación de hacerlo. Si bien existía una suerte de proceso de dos semanas que permitía a la parte demandada presentar alegaciones en contra; sin embargo, dado que las alegaciones resultaban caras para cualquier proveedor de servicios de internet, lo normal es que estos eliminaran el contenido de inmediato permitiendo al autor o a la persona que había subido la información defender su derecho por su cuenta. El efecto de esta ley ha tenido graves consecuencias en Estados Unidos, eliminándose cantidades ingentes de información. La Cienciología la utilizó de manera abusiva

para eliminar literalmente miles de vídeos de You Tube.[7]

Así que aunque demos por sentado que el ACTA ha sido noqueada en el Parlamento Europeo, y eso sea un triunfo en sí mismo, al menos en lo que respecta a este combate, las principales novedades del ACTA parecen seguir aplicándose —hemos mantenido un debate democrático, el ACTA ha sido demonizado en la esfera pública, nuestro discurso ha vencido, pero, entre bambalinas, se siguen firmando tratados bilaterales de carácter secreto que están consiguiendo el mismo resultado, se ha subvertido el proceso democrático. Un ejemplo ilustrativo es el nuevo acuerdo de libre comercio entre la India y Estados Unidos revelado por WikiLeaks, en el que se incorporan prolijos apartados del ACTA.[8] Lo mismo ha ocurrido con gran número de acuerdos y legislaciones. La cabeza del ACTA bien podría llegar a cortarse, pero el cuerpo se partirá en pedazos que acabarán colándose en el orden internacional en forma de tratados bilaterales como éstos. Por tanto, podéis tener vuestras victorias democráticas en público, en la superficie, pero en el fondo las cosas siguen haciéndose de la misma manera. Esto explica por qué no creo que la política o la reforma legislativa sea el camino; aunque tampoco se les puede dar vía libre, pues eso aceleraría el proceso. Así que es importante inspeccionarlos de múltiples modos, como se está inspeccionando el ACTA. Esto los ralentiza. Con todo, un

triunfo en el Parlamento desestimando su regulación no detiene su actividad subrepticia.

JACOB

Una de las cosas que creo que hay que apuntar es que Roger Dingledine, uno de los creadores de Tor, de quien diría que ha sido para mí una especie de mentor que me ha dado mucho que pensar con respecto a la elusión de la censura y el anonimato en la red, habla sobre cómo, por ejemplo, los cortafuegos no son técnicamente efectivos —y es importante entender la tecnología que hay detrás si quieres construir tecnología que los resista—, pero sí son efectivos socialmente. La gente que lucha contra el ACTA está usando esta tecnología y les capacita para resistir, sin embargo aquí lo que hay que entender son los medios de la gente de a pie y no el argot técnico. Lo que importa es que la gente se implique en esa narrativa y la cambie mientras tenga el poder para hacerlo, y el aspecto humano es, de hecho, la parte más importante. WikiLeaks ha revelado documentos que lo hacen posible, y el intercambio de información es clave, pero también lo es la gente que adquiere esa información y la mueve. Porque, al menos en teoría, muchos de nosotros vivimos en democracia, somos libres, y se supone que nos gobiernan con nuestro consentimiento Así que si todo el mundo entendiera lo que está pasando, y se diera cuenta de que no es algo que consintamos, entonces sería muy difícil seguir adelante y aprobar tales acuerdos

con rango de ley, y hacerlo sin el consentimiento de aquellos que son gobernados.

JÉRÉMIE

Todo consiste en incrementar el coste político de adoptar esas malas decisiones para aquellos que las toman. Y podemos hacerlo colectivamente con una internet libre, siempre y cuando la tengamos en nuestras manos.

JACOB

Pero también podrías hacerlo sin internet, porque, históricamente, hemos tenido sociedades libres pre-internet, sólo era más caro económicamente, más difícil en algunos aspectos, de ahí la importancia del movimiento P2P.[9]

ANDY

Creo que el cuarto punto radica en que la dimensión arquitectónica de los sistemas descentralizados es una pieza fundamental que también necesita ponerse en manos de la gente, porque ahora tenemos el fenómeno centralizado de la computación en la nube o *cloud computing*.[10]

JULIAN

Tenemos la red social de Facebook completamente centralizada. La de Twitter, completamente centralizada. A Google, completamente centralizado. A todos los habitantes

de Estados Unidos, todos, bajo el control de quienquiera que controle la fuerza coercitiva. Es como la censura que surgió inmediatamente después de que WikiLeaks sacara los documentos del *Cablegate*, cuando Amazon eliminó nuestro sitio web de sus servidores.[11]

ANDY

Y tenemos la informática en la nube ofreciendo un incentivo económico para que las empresas tengan un modo más barato de procesar sus datos en los denominados centros internacionales de datos gestionados por compañías estadounidenses, lo cual se traduce en trasladar información a las jurisdicciones de Estados Unidos, igual que las compañías de pago y demás.

JULIAN

Hay una tendencia en este cambio hacia el *cloud computing* que resulta preocupante. Hay enormes clúster/conglomerados de servidores ubicados en el mismo sitio, pues es la manera más eficiente de estandarizar el control del entorno, de estandarizar el sistema de pago. Es una técnica competitiva, porque acumular servidores en la misma ubicación es más barato que tenerlos repartidos por ahí. La mayor parte de las comunicaciones que se establecen en internet, salvo en el caso de las películas en *streaming*, son de servidor a servidor, así que cuanto más cerca estén

colocados los servidores más barato será. Y el resultado son estas grandes colmenas de servidores de comunicación. En el caso de Google, por ejemplo, tiene sentido que coloque sus servidores cerca de los grandes proveedores de contenidos o viceversa, porque Google indexa las páginas de manera que puedan ser consultadas. De modo que existen enormes edificios en Estados Unidos atestados de servidores pertenecientes a distintas compañías. Ahí es donde la Agencia de Seguridad Nacional coloca sus «puntos de recogida» de toda su interceptación masiva. Internet podría existir perfectamente sin esta centralización, no es que sea imposible tecnológicamente, simplemente es más eficiente tenerlo todo centralizado. En la competición económica, la versión centralizada se lleva la palma.

ANDY

Si bien es importante entender la perspectiva de la arquitectura —las infraestructuras centralizadas facilitan sobremanera el control central y el abuso de poder—, esto es como matar al pequeño supermercado de al lado con una idea de comercio minorista centralizado.

JULIAN

Y pasar a una grandísima multinacional como Safeway.

ANDY

Sí, lo mismo ocurrió con las compras. Es muy importante mantener un enfoque estructural descentralizado. Cuando yo formaba parte de ICANN, la Corporación de Internet para Nombres y Números Asignados, encargada de asignar y regular los nombres de dominio en Internet, aprendí algo de Vince Cerf, inventor de al menos una parte del protocolo TCP/IP, el protocolo de comunicación más importante de internet. Él siempre solía decir: «Sabes, una cosa buena de los gobiernos es que nunca son singulares, siempre son plurales». Así que incluso entre los gobiernos, siempre están aquellos que quieren su propio ámbito de poder descentralizado, e incluso en el seno de los propios gobiernos existen diversas facciones que luchan entre sí. Eso es lo que en última instancia nos salvará del Gran Hermano, porque habrá demasiados queriendo ser el Gran Hermano y acabarán enzarzándose unos con otros.

JULIAN

Lo dudo, Andy. Creo que en el pasado tuvimos élites nacionales que competían entre sí, y ahora se están asociando unas con otras al tiempo que se desvinculan de sus respectivas poblaciones.

ANDY

Se están asociando, tienes razón en ese punto —y dudo mucho que eso nos vaya a salvar el culo—, pero todavía nos queda la opción de mantener nuestra identidad.

Tenemos que aferrarnos a nuestra propia infraestructura, eso es lo más importante que tenemos que aprender aquí: que si queremos enfrentarnos al Estado de vigilancia, al Gran Hermano, tenemos que estudiar su estructura, si realmente se trata de una asociación de las principales potencias que dicen: «Eh, si nos unimos podemos ganar todavía más». Y nosotros necesitamos saber cuál es nuestro papel aquí, nuestro rol es mantenernos descentralizados, tener nuestra infraestructura propia y no confiar en la informática en la nube y toda esa basura, tener nuestro espacio.

JULIAN

El caso es que aunque podamos dominar la técnica, es un hecho que es más fácil usar Twitter que crear tu propio Twitter; es un hecho que es más fácil usar Facebook que DIASPORA, o una red alternativa; es un hecho que la informática en la nube es más barata, y por ende es evidente que estas técnicas y servicios tienen el poder.[12] No se trata de decir que deberíamos crear nuestros propios servicios locales, porque estos servicios locales nunca serán competitivos, pues sólo serán utilizados por una minoría. Necesitamos plantear algo mejor que la opción de ser el hermano pobre de Facebook y esperar que la gente la utilice.

ANDY

Bueno, retomando la analogía de la Iglesia católica,

estamos retrocediendo a los tiempos en que sólo había un emisor de libros, pues Amazon trata de controlar toda la cadena de producción de los libros digitales, así que nosotros deberíamos mantener nuestra propia capacidad de impresión y publicación. Esto puede sonar un poco exagerado, pero ya hemos visto lo que este tipo de compañías puede hacer si ellas o las agencias gubernamentales de las que dependen no quieren que salga determinada información. Y creo que el siguiente paso necesario será evidentemente que contemos con nuestro propio dinero, de modo que aunque no les guste el hecho de que apoyemos proyectos como WikiLeaks u otros, podamos hacerlo sin tener que depender de ninguna infraestructura central enmarcada en una jurisdicción determinada.

JÉRÉMIE

Me gustaría estar de acuerdo con Andy. Creo que la arquitectura importa y es fundamental para aquello que defendemos. Pero este es un mensaje que debemos transmitir al público, es nuestra responsabilidad, porque nosotros, como hackers, como técnicos que construimos e interactuamos con internet a diario, lo entendemos. Y tal vez sea este el modo de ganarnos los corazones y las mentes de las generaciones más jóvenes. Creo que ahí radica la importancia de las guerras de derechos de autor, porque con las tecnologías P2P, desde Napster en 1999, la gente empezó

a entender —lo pilló— que intercambiando archivos entre individuos...

JULIAN

Te conviertes en criminal.

JÉRÉMIE

No, construyes una cultura mejor.

JULIAN

No, eres un criminal.

JÉRÉMIE

Ésa es la historia que te cuentan, pero si construyes una mejor cultura para ti mismo, todo el mundo usará Napster.[13]

ANDY

La historia de la raza humana y la historia de la cultura es la historia de copiar pensamientos, modificarlos y procesarlos una y otra vez, si tú llamas a eso robar eres un cínico más.

JÉRÉMIE

Exacto, ¡eso es! Es consustancial a la cultura que ésta se comparta.

JULIAN

Bueno, en Occidente desde la década de los cincuenta hemos tenido la cultura industrial. Nuestra cultura se ha convertido en un producto industrial.

JÉRÉMIE

Estamos alimentando al trol, porque está haciendo de abogado del diablo y lo está haciendo muy bien.

JACOB

Yo no pico. Es una absoluta gilipollez.

JÉRÉMIE

Es una gilipollez. En el discurso político se llama robar, pero quiero dejar claro que todos aquellos que usaron Napster en 1999 acabaron haciéndose fans de la música y luego fueron a conciertos y se convirtieron en prescriptores al decir a todo el mundo: «Deberías escuchar a esta gente, deberías ir a tal concierto». Así que la gente ha tenido un ejemplo práctico de cómo la tecnología P2P descentralizó la arquitectura. De hecho, Napster estaba un poco centralizado en aquella época, pero sembró la idea de una arquitectura descentralizada. Todo el mundo tenía un ejemplo concreto que demostraba que la arquitectura descentralizada era buena para la sociedad y, si lo era para compartir cultura,

también es bueno para compartir conocimiento. El intercambio de conocimiento es en suma lo fundamental cuando debatimos cómo sortear la censura o cómo erradicar la narración política para construir un sistema democrático y una sociedad mejores.

Por tanto, tenemos ejemplos que confirman que los servicios descentralizados y el intercambio de información entre individuos mejoran las cosas; y el ejemplo contrario es el del abogado del diablo representado por Julian, donde una industria llega y dice: «Oh, esto es robar y esto es matar a todo el mundo, matar a los actores, matar a Hollywood, matar el cine y a todo lo demás». Ellos han ganado batallas en el pasado y ahora puede que nosotros estemos a punto de ganar la batalla del ACTA. Y de nuevo tengo que expresar mi desacuerdo con el abogado del diablo que Julian estaba representando hace un momento. El ACTA ha sido el mayor ejemplo conocido de elusión de la democracia, pasando por encima del Parlamento y de las instituciones internacionales, pasando por encima de la opinión pública e imponiendo medidas inaceptables por la puerta de atrás. Si conseguimos derrocarlo, entonces sentaremos un precedente, y tendremos la oportunidad de impulsar una agenda constructiva, decir: «El ACTA se ha acabado, ahora hagamos algo que realmente favorezca al público». Y nosotros estamos trabajando en ello, y algunos miembros del Parlamento Europeo ahora entienden que cuando los

individuos comparten cosas, cuando comparten archivos sin un beneficio, no deberían ir a la cárcel, no deberían ser castigados. Creo que si conseguimos que esto cale en el Parlamento, tendríamos un sólido argumento para exponer al resto del mundo que el hecho de compartir conocimiento, el intercambio de información, ayuda a mejorar las cosas, que tenemos que promoverlo en lugar de combatirlo y que cualquier intento —ya sea legislativo o por parte de un dictador o de una empresa— de mermar nuestra capacidad de compartir información y conocimiento de manera descentralizada debe ser combatido. Creo que podríamos dar un gran salto.

JULIAN

¿Y qué hay del debate PIPA/SOPA en Estados Unidos? Son propuestas de ley planteadas en el Congreso de Estados Unidos para crear embargos financieros y bloqueos de internet en beneficio de las industrias estadounidenses.

JACOB

Se creó concretamente para atacar a WikiLeaks y a todo aquello que tuviera que ver con WikiLeaks o fuera afín a WikiLeaks.

JULIAN

En el Congreso se mencionó específicamente el bloqueo

bancario efectuado contra nosotros como una herramienta eficaz.[14]

JÉRÉMIE

Y lo siguiente era dar esta herramienta a Hollywood.

JULIAN

Así que orquestamos una gran campaña comunitaria en su contra, a la que finalmente acabaron uniéndose Google, Wikipedia y otras compañías. Pero yo no participé. «Vale, genial, hemos ganado la batalla.» El caso es que me entró miedo, porque Google de pronto se vio a sí misma como un actor político y no sólo como distribuidora, y sintió el tremendo, el enorme poder que tenía sobre el Congreso.

JÉRÉMIE

Google era sólo una pequeña parte de la coalición anti-SOPA/PIPA.

JACOB

Sí, pero espera un momento, creo que Tumblr tuvo aún más impacto del que tuvo Google.

ANDY

Tumblr y Wikipedia y toneladas de acciones individuales, acciones muy pequeñas de las que no sabemos

nada, tuvieron su impacto. Hubo miles de ellas que fueron paralizadas, todas en una misma dirección —y eso es, de nuevo, acción política descentralizada. Hemos sido testigos de un movimiento político descentralizado. Google ha sido el principal actor que habéis advertido, pero hubo otros muchos.

JULIAN

Bueno, es lo que el Congreso declaró haber advertido.

JACOB

Yo discrepo un poco con lo que Jérémie dijo antes, porque tú básicamente fomentas la idea de una vanguardia política. No creo que fuera eso lo que querías decir, pero lo has dicho, y quería detenerte justo ahí, porque el movimiento P2P está explícitamente en contra de una vanguardia política. Se basa en la idea de que todos somos iguales y podemos compartir e intercambiar información entre nosotros; en que todos podemos ofrecer distintos servicios o distintas funcionalidades. Una vez Ross Anderson me dijo: «Cuando me uní al movimiento P2P hace 50 años...» Y a mí me pareció un comienzo fantástico. Me explicó que quería asegurarse de que nunca «desinventáramos» la imprenta. Porque a medida que empezamos a centralizar servicios, a medida que empezamos a centralizar el control de los sistemas de información, de

hecho empezamos a «desinventar» la imprenta en el sentido de que la enciclopedia británica deja de imprimir libros y sólo imprime CDs —si careces de un ordenador de uso general que pueda leer esos CDs, no tienes acceso a ese conocimiento—. Actualmente el caso de la enciclopedia británica no tiene mayor importancia porque tenemos Wikipedia y gran cantidad de material. Sin embargo no creo que como sociedad estemos preparados.

ANDY

No creo que Wikipedia sea tan buena como fuente de consulta. No me fío de una sola página que no haya tenido que reescribir yo mismo.

JACOB

Pero la enciclopedia británica no es diferente. Es una fuente más, y lo que importa es la verificación de la información. Todo lo que quería decir es que no deberíamos promover esta idea de una vanguardia porque es muy peligrosa.

JULIAN

Espera un momento. ¿Por qué? Yo formo parte de una vanguardia. ¿Qué problema tienes con ellos?

JÉRÉMIE

No estoy hablando de vanguardias, sólo estoy diciendo que tenemos nuevas herramientas en nuestras manos. Hemos mencionado la imprenta. Otro visionario, mi amigo Benjamin Bayart, tal vez menos conocido fuera del mundo franco-parlante, decía: «La imprenta enseñó a la gente a leer; internet enseñó a la gente a escribir».[15] Esto es algo extremadamente novedoso, esto es una nueva capacidad para que todo el mundo pueda escribir y expresarse.

ANDY

Sí, pero filtrar es cada vez más importante.

JÉRÉMIE

Claro, porque todo el mundo habla, y muchos no dicen más que gilipolleces. Como seguramente te diría el académico y activista Larry Lessing e, imagino, también muchos profesores: enseñamos a la gente a escribir pero cuando los estudiantes nos entregan sus ejercicios, el 99 coma algo por ciento son basura, y a pesar de todo les enseñamos a escribir.[16] Así que, por supuesto, la gente dice gilipolleces en internet —eso es evidente—. Sin embargo el mero hecho de poder usar esta capacidad para expresarte en público te ayuda con el tiempo a elaborar más y más tu manera de expresarte, y a participar cada vez con mayor asiduidad en debates complejos. Además, todos los fenómenos que estamos describiendo están construidos

alrededor de una complejidad ingenieril que necesitamos desglosar en pequeñas partes, con el fin de entenderlas y poder debatirlas con calma. La solución no es una vanguardia política, sino canalizar a través del sistema político esta nueva capacidad para expresarnos que todos tenemos a nuestro alcance, para compartir pensamientos, para participar en el intercambio de conocimiento sin necesidad de pertenecer a un partido político, a una agencia de comunicación o a cualquier otra estructura que en el pasado necesitábamos para hacernos oír.

Internet y la economía

JULIAN

Quiero echar un vistazo a las tres libertades básicas. Cuando entrevisté al líder de Hezbollah, Hassan Nasrallah...

JACOB

¿Dónde está el jodido ataque de los *drones*? ¿Qué pasa ahí arriba?

JULIAN

Bueno, él también sufre su particular arresto domiciliario porque no puede abandonar el lugar donde se esconde.

JACOB

No sé si es la comparación más acertada. Por favor no hagas esa comparación.

JULIAN

Cabe preguntarse si Hezbollah tiene los ingredientes de un Estado ¿Se ha convertido realmente en un Estado? Esto es algo que se mencionaba en los cables de la Embajada estadounidense, que Hezbollah ha desarrollado su propia red de fibra óptica en el sur del Líbano.[1] De modo que cuenta con los tres ingredientes primordiales de un Estado: tiene el control de una fuerza armada en una región concreta, dispone de una infraestructura de comunicaciones que controla, y cuenta con una infraestructura financiera. Asimismo, también podemos plantear esto como las tres libertades básicas. La libertad de movimiento, la libertad física de movimiento: la capacidad de movernos de un sitio a otro sin tener un ejército pisándonos los talones. En segundo lugar podemos pensar en la libertad de pensamiento y en la libertad de comunicación, la cual es inherente a la libertad de pensamiento: si sufres amenazas por expresarte públicamente, la única manera de salvaguardar tu derecho a comunicarte es comunicarte privadamente. Y finalmente, la libertad de interacción económica, que al igual que la libertad de comunicación, también está indisolublemente unida a la privacidad de la interacción económica. De modo que hablemos de estas ideas que desde la década de los noventa se han venido gestando en el movimiento criptopunk con el fin de conseguir la importantísima tercera libertad, la libertad de

interacción económica.

JÉRÉMIE

¿Pero por qué necesitarías sólo tres libertades? En mi Carta Europea de Los Derechos Fundamentales hay más.

JULIAN

La privacidad es fundamental tanto desde una perspectiva comunitaria, que básicamente implica que necesitas privacidad para comunicarte y pensar libremente, como desde una perspectiva económica, pues en cierto sentido la necesitas para interactuar económicamente. Por eso creo que aunque existen más libertades derivadas, éstas que he mencionado son las tres libertades fundamentales que originan todas las demás.

JÉRÉMIE

Bueno, ya existe una definición legal para el término libertad fundamental.

JULIAN

Pero yo he leído la Carta de la Unión Europea y te aseguro que eso es un auténtico batiburrillo para el consenso.

JÉRÉMIE

Sí, de acuerdo, y los lobbies consiguieron incluir la

propiedad intelectual en la Carta.

JULIAN

Todo tipo de barbaridades.

ANDY

Estoy convencido de que hay un punto en el que todos estamos de acuerdo: en que el sistema monetario, la infraestructura para intercambiar dinero que tenemos a día de hoy, es un asco. Cualquiera que tenga una cuenta en eBay nos dará la razón, porque lo que Paypal está haciendo, lo que Visa y MasterCard están haciendo, es poner a la gente en una situación de monopolio de facto. También estaba ese asunto tan interesante mencionado en los cables filtrados por WikiLeaks, el que apuntaba que el gobierno ruso trataba de negociar un modo para que los pagos efectuados con Visa y MasterCard por ciudadanos rusos en territorio ruso fueran procesados en Rusia, y respecto al que Visa y MasterCard se negaron.[2]

JULIAN

Sí, el poder combinado de la Embajada estadounidense y de Visa fue suficiente para evitar que Rusia implantara su sistema nacional de pago con tarjeta en su territorio.

ANDY

Eso significa que incluso los pagos de los ciudadanos rusos entre negocios rusos serán procesados a través de los centros de datos americanos. Entonces el gobierno estadounidense tendrá control jurisdiccional, o al menos conocimiento ¿cierto?

JULIAN

Exacto, así que cuando Putin sale a comprar una Coca-cola, treinta segundos más tarde se sabe en Washington DC.

ANDY

Y eso, por supuesto es una situación muy incómoda, independientemente de que me guste o no Estados Unidos. Es sumamente peligroso tener un único centro de datos donde se almacenan todos los pagos, porque eso invita a todo tipo de usos.

JACOB

Una de las claves que reconoce el movimiento criptopunk es que la arquitectura ciertamente define la situación política, así que si tienes una arquitectura centralizada, aun cuando esté en manos de la mejor gente del mundo, irremisiblemente atrae a los cabrones y estos cabrones hacen cosas con su poder que los diseñadores originales no harían. Y es importante tener claro que todo es cuestión de dinero.

JULIAN

Como los pozos de petróleo de Arabia Saudí, la maldición del petróleo.

JACOB

Miremos donde miremos advertiremos, especialmente en lo que respecta a los sistemas financieros, que aun cuando la gente tiene las mejores intenciones, da lo mismo. La arquitectura es la verdad. Es la verdad de internet con respecto a las comunicaciones. Los denominados sistemas legítimos de interceptación, lo cual no es más que una forma bonita de llamar a los sistemas de espionaje.

JULIAN

La interceptación legal es un eufemismo.

JACOB

Absolutamente, como asesinato legítimo.

ANDY

O tortura legítima.

JACOB

¿Habéis oído hablar de ataques «legítimos» a ciudadanos norteamericanos ejecutados por aviones no tripulados ordenados por el mismísimo presidente Obama?

Cuando mató al hijo de dieciséis años de Anwar al-Awlaki en Yemen se lo llamó asesinato legítimo, o matar al objetivo... Como ellos dicen.[3] La llamada interceptación legítima es lo mismo —simplemente pones la palabra «legítimo» delante de algo y, de pronto, el Estado lo lleva a cabo, es legítimo. Pero en realidad es la arquitectura del Estado lo que les permite hacer todas esas cosas, es la arquitectura de las leyes y la arquitectura de la tecnología, no únicamente la arquitectura de los sistemas financieros.

Lo que los criptopunks querían hacer era crear sistemas que nos permitieran pagarnos los unos a los otros de una forma verdaderamente libre en la que no haya posibilidad de interferir. Como las monedas *chaumianas*, un tipo de divisa electrónica diseñada conforme a las especificaciones de David Chaum, el creador del eCash (una moneda electrónica completamente anónima), aunque tal vez habría que decir que está más centralizada de lo necesario. La idea es poder crear divisas anónimas opuestas a Visa y MasterCard, que son en realidad monedas de rastreo o seguimiento. La moneda *chaumiana*, aunque está construida en torno a una autoridad concreta, utiliza protocolos criptográficos inventados por David Chaum para garantizar el anonimato en cualquier tipo de transacción.[4]

JULIAN

Entonces es básicamente efectivo electrónico sin,

digamos que, números de serie en el efectivo.

JACOB

O con números de serie que te permiten establecer que se trata de una moneda válida pero que a la vez impiden que sepas si Julian pagó a Andy o el importe pagado.

JÉRÉMIE

Es algo como recrear el efectivo del mundo real en el mundo digital.

JULIAN

Crear una moneda electrónica es un gran reto precisamente porque el control sobre sistema monetario es uno de los tres ingredientes de un Estado, como ya he dicho al hablar de Hezbolla. Si eliminas este monopolio estatal sobre los medios de interacción económica, entonces eliminas uno de los tres componentes del Estado. En el modelo de Estado concebido como una mafia, el Estado ejerce de extorsionador, registrando a las personas en busca de dinero de todos los modos posibles. Controlar los flujos de divisas es importante para incrementar los ingresos del Estado, pero también para controlar lo que la gente hace: incentivar una cosa, desincentivar otra, prohibir totalmente ciertas operaciones, o una organización, o las interacciones entre organizaciones. De modo que, por ejemplo, lo que ocurrió con el insólito bloqueo a WikiLeaks no fue fruto de

una decisión del libre mercado, pues no tenemos un libre mercado: las legislaciones estatales han convertido a determinados actores financieros en reyes y no permiten la entrada de nuevos actores. La libertad económica ha sido vulnerada por una élite capaz de influir tanto en la normativa como en los principios que rigen estos bancos.[5]

ANDY

Lamentable, éste es el problema no resuelto del mundo electrónico ahora mismo. Dos compañías de crédito, ambas con infraestructura electrónica ubicada en Estados Unidos con vía libre para operar —lo cual significa acceso a toda la información en la jurisdicción estadounidense—, controlan la mayoría de los pagos efectuados con tarjeta de crédito del planeta. Compañías como Paypal, que también se ampara en la jurisdicción norteamericana, aplica políticas estadounidenses, ya sea en el bloqueo de la venta online de puros cubanos por parte de minoristas alemanes o en el bloqueo de pagos a WikiLeaks en jurisdicciones no estadounidenses. Esto significa que el gobierno de Estados Unidos tiene acceso a la información y la opción de imponer controles de pago sobre pagos efectuados en todo el mundo. Mientras que los ciudadanos americanos pueden argüir que ésta el la mejor democracia que el dinero puede comprar, para los europeos simplemente no tiene precio.

JULIAN

En el mundo tradicional que conocemos hemos tenido una relativa libertad de movimiento, aunque en algunos casos no era tanta.

JACOB

¿Estás seguro, Julian? Tengo la sensación de que tu libertad de movimiento es el ejemplo clásico de lo libres que somos en realidad.

JULIAN

Bueno no, el Reino Unido ha anunciado que va a poner cien mil personas al año en mis mismas condiciones.[6] Así que creo que lo mío es en cierta medida un efecto colateral.

JACOB

Éste es el motivo por el cual los fundadores de mi país disparaban a la gente de Gran Bretaña. ¡Ytodavía existe hoy! La tiranía existe.

JÉRÉMIE

No llevemos el tema a lo personal.

ANDY

Lo que tu país, Estados Unidos, está haciendo actualmente es privatizar cárceles y negociar contratos que

garantizan un 90 por ciento de ocupación a las compañías privadas que se encarguen de estas antiguas prisiones gubernamentales.[7] Bien, ¿Y esto qué es? Es el absurdo del capitalismo en grado sumo.

JULIAN

Hay más presos en las cárceles estadounidenses que los que hubo en la antigua Unión Soviética.

JACOB

Eso es una falacia en la que, como yo argumento que algo está mal, tú sugieres que yo formo parte de algo que también está mal. No estoy diciendo que Estados Unidos sea perfecto. Creo que Estados Unidos es un país estupendo en muchos sentidos, pero especialmente en lo que respecta a la retórica de los Padres Fundadores.

JULIAN

La retórica de los Padres Fundadores se está desintegrando desde hace diez años.

JACOB

No olvidemos que gran parte de la visión que existe sobre la retórica de los Padres Fundadores es mitología y que debemos ser cautelosos a la hora de idealizarlos. Por tanto, sí, claro, eso salta a la vista. Lo que yo quería decir

con el comentario sobre la tiranía de los británicos y la situación en que Julian se encuentra es que todo se debe a una cuestión cultural. Aquí es donde la sociedad entra en juego, y donde deviene importantísima, y es muy difícil para la tecnología suplantar ese papel. Y los asuntos económicos son el problema más peliagudo que debemos resolver. Por eso la persona que creó una moneda electrónica alternativa, el Bitcoin, lo hizo de un modo tan anónimo. Nadie quiere ser la persona que inventa la primera moneda electrónica realmente exitosa.[8]

JULIAN

Los tíos que inventaron el oro electrónico acabaron siendo procesados en Estados Unidos.[9]

JACOB

Es increíblemente frustrante.

JULIAN

Volvamos al tema de estas tres libertades fundamentales: la libertad de comunicación, la libertad de movimiento y la libertad de interacción económica. Si observamos la transición de nuestra sociedad global a internet, cuando hicimos esa transición la libertad de movimiento seguía siendo, en esencia, la misma. La libertad de comunicación mejoró sobremanera en el sentido de que ahora podemos comunicarnos con mucha más gente; sin

embargo, por otro lado, también se ha visto tremendamente degradada, porque ya no existe la privacidad, y por consiguiente nuestras comunicaciones pueden ser espiadas y almacenadas, como de hecho sucede, para eventualmente utilizarse en nuestra contra. De modo que esa interacción elemental que tenemos con la gente físicamente se ha degradado por completo.

ANDY

La privacidad es posible, pero tiene un precio.

JULIAN

Nuestras interacciones económicas han sufrido exactamente las mismas consecuencias. De tal forma que en una interacción económica tradicional ¿quién se enteraba? Aquellos que te veían ir al mercado. Ahora ¿quién se entera de tu interacción económica? Si compras algo al vecino de al lado con tu tarjera Visa, cosa que en la sociedad de mercado tradicional sería prácticamente privada, ¿quién se entera ahora?

JACOB

Todo el mundo.

JULIAN

Todo el mundo. Las principales potencias occidentales

controlan entre sí el intercambio de información, todas tienen conocimiento de esta información y la almacenan para siempre.

ANDY

Julian, no es que no tengas razón en lo que planteas, pero no estoy seguro de que se pueda distinguir entre la libertad de comunicación y la libertad de interacción económica, porque lo cierto es que internet, tal como la conocemos ahora, es la infraestructura para nuestras interacciones sociales, económicas, culturales y políticas, para todas nuestras interacciones.

JACOB

Todo redunda evidentemente en la libertad de movimiento.

ANDY

Independientemente de cuál sea la libertad de comunicación, el dinero se reduce a bits. Éste es el principal uso de internet. De modo que si el sistema económico está basado en la infraestructura electrónica, la arquitectura de la infraestructura electrónica tiene algo que decir sobre cómo se produce el flujo de dinero, sobre cómo está siendo controlado y cómo está siendo centralizado. Tal vez en sus inicios ni siquiera se pensaba que internet fuera a ser la

infraestructura para todo a día de hoy, pero la lógica económica dijo: «Bueno, es más barato hacer tal cosa con internet». Los bancos y las compañías de tarjetas antes tenían cajeros automáticos ahí fuera con interfaces X.25, que constituían una red autónoma hace diez o veinte años, y ahora todo se rige por el modelo TCP/IP, porque es más barato.[10] Por tanto la arquitectura de la tecnología se ha convertido en un asunto clave, pues afecta a todos los demás campos, y eso es lo que realmente tenemos que redefinir, en el sentido de que si queremos contar con un sistema descentralizado de gestión de nuestros pagos, necesitamos tener la infraestructura en nuestras manos.

JACOB

Bitcoin es básicamente una moneda electrónica.

ANDY

Sin inflación.

JACOB

Su objetivo es operar de manera descentralizada, de modo que en lugar de tener una Reserva Federal tienes un grupo de personas repartido por el mundo que deciden cuál es su realidad y cuál es su moneda vigente.

JULIAN

Y existen algunos programas informáticos que ayudan a hacerlo posible.

JACOB

Quiero explicarlo en palabras no técnicas. Se trata de una moneda electrónica que funciona más como una mercancía que como una moneda, y sobre la que la gente decide a cuántos euros equivale un Bitcoin. De modo que es un poco como el oro a este respecto. Por otro lado está el coste de la llamada minería de Bitcoins, donde tú haces una búsqueda en un ordenador para encontrar un Bitcoin, y la idea es que hay una complejidad computacional a la que se vincula el valor de la mercancía. Dicho de otro modo, es una forma de que yo pueda transferir dinero a Julian y de que Julian acuse recibo del envío sin que Andy pueda en ningún caso interferir o impedir la operación. Sin embargo existen algunos problemas, pues en realidad no es una moneda anónima, y creo que esto es algo muy perjudicial.

JULIAN

El Bitcoin es un híbrido muy interesante, pues los titulares de las cuentas son completamente privados, y cualquiera puede abrirse una cuenta cuando quiera, sin embargo las transacciones en la economía del Bitcoin son completamente públicas. Y así es como funciona, tiene que ser así para que todo el mundo acepte que una transacción

ha sido efectuada, para que todos sepan que, desde ese preciso momento, la cuenta del remitente tiene menos dinero y la cuenta del destinatario tiene mucho más. Ése es uno de los modos de operar un sistema distribuido de moneda que no requiere de un servidor central (sin duda un objetivo tentador para el control coercitivo). Lo realmente innovador en el Bitcoin es la distribución y los algoritmos que permiten dicha distribución, donde tú no confías, por así decir, en ninguna parte específica de la red bancaria del Bitcoin. Más bien la confianza está distribuida. Y su correcta ejecución no se regula a través de leyes, reglamentos o auditorías, sino a través de la dificultad criptográfica computacional que cada parte de la red debe afrontar para demostrar que realmente está haciendo lo que dice estar haciendo. De modo que la ética *bancaria* del Bitcoin está integrada en la arquitectura misma del sistema. La computación se traduce en costes de electricidad para cada una de las ramificaciones del banco Bitcoin, de tal forma que podemos asignar un coste a la comisión de un fraude atendiendo al precio de la electricidad. El trabajo requerido para cometer un fraude está originalmente diseñado para acarrear mayores costes de electricidad que el beneficio económico derivado del mismo. Es algo muy innovador, no porque estas ideas no se haya explorado antes (llevan sobre el papel más de veinte años), sino porque el Bitcoin consiguió un equilibrio casi perfecto e introdujo una idea muy novedosa sobre cómo probar un

verdadero consenso global sobre las transacciones de la economía Bitcoin, asumiendo incluso que muchos bancos eran fraudulentos y que cualquiera podía crear el suyo propio.

Por supuesto, igual que sucede con cualquier otra moneda, tienes que comprar la moneda con algo más; con trabajo, o los Bitcoins se cambian por otra moneda —existen grupos de intercambio de divisas que se encargan de ello. Existen también otras limitaciones. Tiene alrededor de diez minutos de plazo de liquidación —se requiere unos diez minutos de trabajo computacional desde que la moneda se transfiere hasta que la otra parte se asegura de que existe un consenso global sobre la transacción efectuada. Es exactamente igual que el efectivo, así que es tan susceptible de robos como el dinero físico. Pero también tiene todas sus ventajas: una vez lo recibes, tienes la certeza de que te han pagado, el cheque no puede cancelarse, el banco no puede revocarlo. Se cortan de cuajo las relaciones de fuerza coercitiva. Por otro lado, tenemos que custodiar bien el efectivo. Ése es, en mi opinión, el mayor problema. No obstante es fácil construir capas adicionales encima, construir servicios de depósito especialmente diseñados para almacenar tus Bitcoins, y mantenerlos a salvo de robos.

JACOB

Curiosamente, si la gente que creó el Bitcoin hubiera

decretado el uso de Tor, de modo que en lugar de tener que crear una cuenta pudieras utilizar algunos identificadores criptográficos, habría sido posible, si todo pasara por Tor como estructura base, que la gente disfrutara de un anonimato de ubicación, aun cuando existieran identificadores a largo plazo que te identificaran a fin de poder vincular todas tus transacciones.

JÉRÉMIE

Sin entrar en consideraciones técnicas podríamos coincidir en que el Bitcoin incorpora algunos conceptos excelentes, pero también algunas imperfecciones. Tiene una naturaleza deflacionista, porque el dinero tiende a desaparecer del Bitcoin. Por tanto aunque no puede funcionar a largo plazo, sí plantea conceptos susceptibles de mejora. Puede que ya vayamos por la versión 0.7 o 0.8.

JACOB

Es como David Chaum reinventado.[11]

ANDY

Diría que el Bitcoin ha sido el intento más exitoso de introducir una moneda digital de la última década.

JULIAN

Consiguieron un equilibrio casi perfecto. Creo que el

Bitcoin continuará. Es una moneda eficiente; puedes crear una cuenta en diez segundos, y para transferir dinero no hay más gasto que el coste derivado de la conexión a internet y unos pocos minutos de electricidad. Es altamente competitivo en comparación con prácticamente todas las formas de transferencia conocidas. Creo que prosperará. Acordaos de lo que pasó tras los robos de Bitcoins y los subsiguientes comentarios negativos de la prensa en el verano del año 2011, la tasa de cambio cayó a tres dólares americanos.[12] El Bitcoin ha subido gradualmente a 12 dólares. No ha sufrido drásticas bajadas o subidas, sino que su ascenso ha dibujado una curva gradual que pone de manifiesto la gran demanda que existe de esta moneda. Sospecho que gran parte de la demanda es puro tráfico de drogas, pedidos de marihuana y esas historias.[13] Pero el hecho es que el Bitcoin comporta pocos gastos como moneda. Varios proveedores de servicios de internet, especialmente en lugares con difícil acceso a las prestaciones que ofrecen las tarjetas de crédito, como la antigua Unión Soviética, están empezando a usarlo.

Sin duda habrá medidas represivas si continúa creciendo. Pero eso no acabará con el Bitcoin, pues la criptografía impide que cualquier ataque a través de la fuerza coercitiva pueda funcionar. No obstante, el tipo de servicios de cambio de divisas que trabajan con el Bitcoin podrían ser identificados mucho más fácilmente. Por otro lado, estos

cambios de moneda pueden operar en cualquier sitio del mundo, así que existen unas cuantas jurisdicciones de las que ocuparse antes de conseguir erradicar estos servicios, y el mercado negro tiene su propia lógica de cambio. Creo que el juego que debe llevarse a cabo con el Bitcoin consiste en que lo adopten los proveedores de servicios de internet y la industria de servicios de internet para estos pequeños juegos que se compran en Facebook y demás, porque es tremendamente eficiente, y una vez se adopte seriamente por un conjunto variado de industrias, estas formarán un lobby para evitar que se prohíba. Así fue en parte cómo se adoptó la criptografía. Solía tildarse de tráfico de armas y a algunos de nosotros nos llamaban traficantes de armas, pero una vez se incorporó a los navegadores y se empezó a utilizar en la banca se formó un lobby lo suficientemente poderoso como para evitar su prohibición —aunque admito que hay nuevas iniciativas en curso.

JACOB

El problema es que las preocupaciones en torno a la privacidad son erróneas. Seamos honestos. Es un error sugerir que el aspecto económico de la situación es diferente con internet y sin internet. Cuando vine compré libras esterlinas y tenía que dar mi número de la seguridad social, que es mi único identificador en Estados Unidos, tuve que dar mi nombre, tuve que asociarlo a una cuenta bancaria y

tuve que darles el dinero. Ellos registraron todos los números de serie y luego cogieron toda esa información y dieron cuenta de ella al gobierno federal. Así que, ésa es la analogía. Y todavía es más difícil conseguir moneda extranjera en Estados Unidos porque nosotros estamos lejos de todos los demás países. El caso es que existe una tendencia histórica de control con relación a la moneda y que este control no se observa sólo en internet. De hecho, tengo entendido que existen cajeros automáticos en los bancos que registran los números de serie de billetes que luego rastrean para hacer análisis de flujos de efectivo y ver dónde se ha gastado y qué se ha hecho con él.

Si observamos esos sistemas y luego echamos un vistazo a internet, no se ha mejorado la privacidad al migrar a la red —de hecho, siguen siendo tan malos como al principio. Por tanto, creo, es importante que veamos las tendencias mundiales que existían antes de internet para poder ver hacia dónde nos dirigimos. Lo que observamos es que si tienes mucho dinero puedes pagar una prima para mantener tu privacidad, y si no lo tienes es prácticamente imposible que lo consigas. Ycon internet es todavía peor. El Bitcoin es un primer paso en la buena dirección, pues si se combinara con un canal anónimo de comunicaciones, como Tor por ejemplo, eso te permitiría enviar a través de Tor un Bitcoin a WikiLeaks y cualquiera que observara esta transacción vería a un usuario de Tor enviándolo y a ti

recibiéndolo. Es posible hacerlo —y eso en muchos sentidos es mucho mejor que el dinero.

JULIAN

Todos hablamos sobre la privacidad de la comunicación y el derecho a publicar. Eso es algo bastante fácil de entender —tiene una larga historia— y, de hecho, a los periodistas les encanta hablar de ello porque están protegiendo sus propios intereses. Sin embargo, si comparamos ese valor con el valor de la privacidad y la libertad de interacción económica, lo cierto es que cada vez que la CIA ve una interacción económica puede ver también quién la efectúa y desde dónde, quién la recibe y desde qué ubicación, así como conocer el valor y la importancia de dicha interacción. De modo que en realidad la libertad o privacidad de las interacciones económicas no es más importante que la libertad de expresión, porque ¿son las interacciones económicas la base real de la estructura de nuestra sociedad?

JACOB

Ambas están intrínsecamente unidas. Creo que aquí radica la diferencia entre los criptopunks americanos y los europeos, ya que la mayoría de los criptopunks americanos diría que ambas libertades son exactamente lo mismo. Porque en una sociedad que tiene un libre mercado cualquiera

alegaría que hay que predicar con el ejemplo, las palabras se respaldan con dinero.

JULIAN

Donde pones tu dinero es donde pones tu poder.

JACOB

Exacto. No digo que eso sea correcto, que esa sea la actitud más apropiada de afrontarlo, puede que no sea eso lo que queremos. Tal vez queramos un capitalismo socialmente limitado, por ejemplo.

JULIAN

Si nos limitamos a verlo desde la perspectiva de los servicios de inteligencia: pongamos por caso que tienes 10 millones dólares de presupuesto para inteligencia, y que te dan la posibilidad de elegir entre espiar las interacciones de la gente a través del correo electrónico o tener un control absoluto de sus interacciones económicas. ¿Qué opción preferirías?

ANDY

Bueno, hoy dirían: «Vale, ya hemos obligado a los bancos y compañías de crédito a usar internet, así que tenemos ambas opciones». Y eso es lo que han hecho. Por tanto la cuestión aquí es que no hay salida. Puedes hacer

cosas como utilizar Tor para proteger tu comunicación, puedes encriptar tus llamadas telefónicas, o enviar mensajes seguros. Pero con el dinero es mucho más complicado, y luego están las llamadas leyes de blanqueo de dinero y demás, y a nosotros nos cuentan que los traficantes y las organizaciones terroristas están abusando de la infraestructura para hacer el mal...

JACOB

Es la película de Los cuatro jinetes del Info-Apocalipsis...

ANDY

Lo cierto es que a mí me interesaría que las empresas de vigilancia y el gobierno fueran más transparentes con respecto a sus gastos. La cuestión es ¿qué estamos comprando realmente cuando nos limitamos a ofrecer anonimato total únicamente en el sistema monetario? ¿Qué podría pasar en realidad? Creo que esto nos podría llevar por interesantes derroteros en los que la gente pueda relajarse más si cabe y decir: «Bueno, ya sabes, puedo alzar mi voz, puedo ir al parlamento, pero también puedo limitarme a comprar a unos cuantos políticos».

JÉRÉMIE

Estás describiendo a Estados Unidos ¿no?

JACOB

No es anónimo.

ANDY

No tengo claro que esto se limite únicamente a Estados Unidos. En Alemania no lo llamamos corrupción, lo llamamos «fundaciones», que compran obras pintadas por las mujeres de los políticos, y así es como funcionan el negocio del arte y otros tantos de diversos sectores. Así que tenemos mejores nombres para ello. Tal vez en Francia lo llaméis «fiestas de la amistad» y otros lo llamen contratar prostitutas.

JÉRÉMIE

El caso de Estados Unidos es especial porque el vínculo entre el sistema político y el dinero es muy estrecho. Larry Lessig declaró, tras diez años trabajando en temas de derechos de autor, que desistía de su intento de regularlos (aunque lo cierto es que no desistió), porque se dio cuenta de que el problema no era que los políticos entendieran en qué consistía una buena política de derechos de autor, el problema era simplemente que había demasiados lazos con los actores industriales que estaban presionando en aras de un mal régimen de derechos de autor.[14] Así que tenemos un verdadero problema con esto.

JULIAN

¿Estás seguro de que es un problema, Jérémie? Puede que, de hecho, sea algo positivo que esas industrias que son productivas...

ANDY

Creo que el abogado del diablo se está bebiendo mi whisky.

JACOB

Veamos si realmente es capaz de terminar la frase sin troncharse de risa. Adelante ¡*Troléanos,* maestro trol!

JULIAN

Esas industrias que son productivas, que generan riqueza para toda la sociedad, utilizan una parte de su dinero para asegurarse de que van a seguir siendo productivas, y lo hacen noqueando cualquier tipo de legislación aleatoria derivada de la creación de mitos políticos sembrados por el bombo publicitario. Y la mejor manera de llevarlo a cabo es, sin duda, comprar a los congresistas, para que hagan el trabajo de su industria productiva y lo utilicen para modificar la ley —para mantener en marcha la naturaleza productiva de la industria.

JACOB

Espera. Eso me lo apunto. ¿Preparados? ¿Listos? Ya ¿Estáis listos? No.

JULIAN

¿Por qué?

JACOB

Por varias razones, pero en concreto porque existe una espiral de retroalimentación que es tremendamente negativa. Por ejemplo, creo que uno de los mayores contribuyentes en la campaña política del Estado de California es la Unión de Guardias Penitenciarios, y esto se debe en parte a las presiones que ejercen como lobby para endurecer las leyes. Y lo hacen no porque les preocupe el Estado de derecho sino porque es un incentivo para este tipo de empleos.[15] De modo que, si ves que esta gente se está uniendo para crear más prisiones, para encarcelar a más gente, para que haya condenas más largas ¿Qué es lo que están haciendo realmente? Lo que están haciendo es utilizar el beneficio que perciben por un trabajo que en principio era beneficioso —aunque tengo mis dudas— para expandir el monopolio que el Estado les garantiza.

JULIAN

Entonces, ¿lo están usando para transferir riqueza de las industrias productivas a industrias que no lo son?

JACOB

Podrías resumirlo así.

JULIAN

Pero puede que eso sea sólo una pequeña pieza. Todos los sistemas sufren abusos, tal vez estos polizones involucrados en la transferencia de riqueza sean un pequeño elemento, y, de hecho, la mayoría de los grupos de presión, la mayor parte de la influencia sobre el Congreso proviene en realidad de industrias productivas, que se aseguran de que las leyes continúen permitiendo su productividad.

JACOB

Pero eso se puede medir muy fácilmente porque siempre puedes averiguar quiénes son los que desean promover actividades de captación de rentas y limitar las libertades de la gente para crear una situación que ni ellos mismos habrían podido alcanzar con su estatus actual. Cuando hacen este tipo de cosas, te das cuenta de que algo ha salido mal y de que se limitan a proteger lo que tienen, lo que han creado básicamente a través de una explotación —por lo general apelando a la emoción cuando declaran: «Dios mío, acabemos con el terrorismo, acabemos con la pornografía infantil, acabemos con el blanqueo de dinero, declaremos la guerra a las drogas». Tal vez esas cosas fueran totalmente

razonables en el contexto original en el que se plantearon, y normalmente lo son, pero, en términos generales, todos pensamos que son cosas malas porque en todas ellas existe un componente grave.

ANDY

Me gustaría retomar tema de los derechos de autor y daros otro ejemplo. Hubo serios problemas cuando los primeros automóviles salieron al mercado. Aquellos que dirigían compañías de transporte de pasajeros con caballos temieron que el invento acabara con su negocio, lo cual era cierto, y tenía su sentido. El caso es que me invitaron a dar a una charla en la asociación de compañías de cine alemán, y justo antes de mi intervención tuvo lugar la de un profesor de la universidad de Berlín que habló correctísimamente sobre la evolución de la raza humana y el desarrollo de la cultura, explicando que el hecho de copiar pensamientos y seguir procesándolos es el factor clave, igual que hacer películas consiste en abordar temas y expresarlos de un modo dramatúrgico. Tras sus cuarenta minutos el moderador le interrumpió descaradamente y dijo: «De acuerdo, tras haberte escuchado hablar en favor de la legalización del robo, veamos lo que tiene que decir el tío del Club del Caos Informático». Y lo pensaba: «¡Guau! ¡Qué demonios! Voy a hablar claro, ¿saldré vivo de aquí?». De modo que algunas industrias simplemente tienen modelos de negocio que no

están contribuyendo a la evolución. Es una postura egoísta, anquilosarse en su afán involucionista, y contribuir a que el monopolio de la industria sea todavía mayor. Cuando se inventaron las casetes también pensaron que la industria discográfica moriría. Sucedió lo contrario, la industria del disco explosionó. La cuestión es ¿cuál sería la política aquí? ¿Cómo podríamos formular este tipo de cosas adecuadamente?

JULIAN

Me pregunto si se podrían estandarizar las prácticas de Estados Unidos y regularse de tal modo que simplemente pudiéramos comprar a los senadores y comprar votos en el senado.

JÉRÉMIE

No, no, no, no.

ANDY

Supongamos que tenemos el dinero para hacerlo.

JULIAN

Sí, y que todo está abierto, y que hay compradores, y que cada uno va a una subasta.

ANDY

Pero la industria armamentística siempre tendrá más dinero.

JULIAN

No, creo que no. Estoy convencido de que el complejo industrial militar quedaría relativamente marginado porque su capacidad para operar a puerta cerrada en un sistema que no está abierto a licitaciones de mercado es superior a la de otras industrias.

JACOB

Hay una palmaria desigualdad en el sistema.

JÉRÉMIE

Desde la óptica liberal y antimonopolística, cuando dices dejemos que los actores dominantes decidan qué política quieren, yo puedo responderte con la experiencia de internet en los últimos quince años, donde existía la denominada innovación «de abajo-a-arriba», donde las nuevas prácticas emergieron de la nada, donde un par de tíos en un garaje inventaron una tecnología que se expandió en todas las áreas.

JULIAN

Para casi todo, para Apple, para Google, para You Tube, para todo.

JÉRÉMIE

Para todo. Todo lo que ha ocurrido en internet ha sido un rotundo éxito pese a ser totalmente desconocido los meses u años inmediatamente anteriores, así que no se puede predecir qué será lo siguiente, y el camino de la innovación es tan rápido que supera con creces al proceso de elaboración de políticas. Por tanto cuando diseñas una ley que tiene un impacto en lo que el mercado es hoy, en la solidez de las relaciones entre las distintas compañías y actores, si refuerzas una que ya sea lo suficientemente fuerte puedes estar frenando la incorporación de nuevos candidatos que tal vez podrían haber sido más eficientes.

JULIAN

Hay que regular el mercado para que sea libre.

JÉRÉMIE

Claro que hay que combatir los monopolios, y necesitas tener un poder superior al de esas compañías para castigar malas conductas. Pero, desde mi punto de vista, la política debe adaptarse a la sociedad, y no al revés. Con las guerras de derechos de autor tenemos la impresión de que el legislador intenta hacer que el conjunto de la sociedad cambie para que se adapte al marco legal definido por Hollywood. Te dicen: «Vale, lo que haces con tu nueva

práctica cultural está moralmente mal. Así que si no dejas de hacerlo, nosotros diseñaremos herramientas legales para impedirte hacer aquello que tú crees que está bien». Ésta no es la forma de hacer política. Una buena política mira al mundo y se adapta a él para corregir lo que está mal y facilitar aquello que está bien. Estoy convencido de que cuando permites que los actores industriales más poderosos del mundo decidan el tipo de política que se debe aplicar, no sigues ese camino.

ANDY

Sólo trato de que todos pensemos constructivamente sobre qué sería una buena política. Lo que acabáis de plantear llegados a este punto es, en mi opinión, demasiado complicado. Trato de simplificar un poco. Heinz von Foerster —el padre de la cibernética— estableció en su día un conjunto de normas, y una de ellas era: «Actúa siempre de tal modo que se incrementen las alternativas».[16] Por tanto, en lo que respecta a la política, la tecnología, lo que sea, haz siempre aquello que te de más, no menos opciones.

JULIAN

Es también la estrategia del ajedrez.

ANDY

Se ha mencionado que el incremento de la privacidad en

las transacciones monetarias puede tener un efecto negativo, así que necesitamos pensar. El sistema monetario tiene actualmente una lógica específica y la pregunta es: ¿cómo impedimos que el sistema monetario se apodere de las demás áreas? Porque el sistema monetario tiene la capacidad —a diferencia del sector de las comunicaciones— de afectar y limitar totalmente las opciones de las personas de otras áreas. Si tú puedes contratar a matones para hacer ciertas cosas, o comprar armas e involucrarte en una guerra con otros países, entonces estás limitando la opción que otras personas tienen de vivir, de actuar. Si yo invierto más dinero en las comunicaciones, esto posibilitará el hecho de que un número mayor de personas tenga más opciones. Si pongo más armas en el mercado...

JACOB

No, cuanta más capacidad de vigilancia tengas, más control tendrás.

ANDY

Lo cual es un argumento más para restringir el mercado armamentístico, incluida la tecnología de vigilancia de las telecomunicaciones.

JACOB

Cierto, quieres restringir mi capacidad para vender ese

tipo de cosas. ¿Y, cómo lo haces? ¿Cómo limitas mi capacidad para transferir riqueza? También a través de las redes de comunicaciones. Uno de los aspectos más ofensivos de los rescates financieros llevados a cabo en Estados Unidos —rescates ofensivos para mucha gente por una larga serie de razones—, fue que demostraron que la riqueza se limita a series/ristras de bits en un sistema informático. Los eficaces ruegos de ciertas personas consiguieron que los bits se pusieran por las nubes, y esto ¿a dónde nos lleva? ¿Existe algún valor en un sistema al que puedes engañar para que suba el precio de tus bits? Y los demás, que tratan de salir adelante, ni siquiera son reconocidos pese a tener bits que merecen intercambiarse en primera instancia.[17]

ANDY

¿Insinúas que lo que necesitamos es un sistema económico totalmente diferente? Porque el valor hoy no está vinculado al aspecto económico.

JACOB

No, lo que digo es que hay un valor económico.

ANDY

Puedes hacer cosas malintencionadas y generar dinero con ello, y también puedes producir cosas buenas y no

ganarás un centavo.

JACOB

Bueno no, lo que digo es que no puedes escindir la economía de la comunicación. No hablo de si necesitamos o no un sistema económico distinto. No soy economista. Sólo quiero decir que existe cierto valor en los sistemas de comunicación y en la libertad de dichas comunicaciones, igual que hay un valor en la libertad de trueque real: yo tengo el derecho de darte algo a cambio de tu trabajo, como también tengo el derecho de exponer una idea y tú tienes derecho a expresar lo que piensas sobre mi idea. No podemos decir que el sistema económico habita en una suerte de vacío. El sistema de comunicación está directamente vinculado a esto, y esto es parte de la sociedad.

Si vamos a tener esta idea reduccionista de la libertad, de las tres libertades que mencionó Julian, esto está evidentemente ligado a la libertad de movimiento —ni siquiera puedes comprar un billete de avión sin usar una moneda rastreable, de lo contrario estás fichado. Si vas a un aeropuerto y tratas de comprar un billete para ese mismo día pagando en efectivo, te fichan. Te aplican medidas extraordinarias de seguridad, no puedes volar sin identificación y, si tuvieras la mala suerte de haber comprado tu billete de avión con una tarjeta de crédito, te registran

todos tus datos, desde tu dirección IP hasta tu navegador. Yo tengo los datos de la Ley de Libertad de Información debido a los registros que sufrí por parte de la Oficina de Inmigración y Control de Aduanas hace un par de años, porque pensé que tal vez algún día sería interesante analizar las divergencias. Como también tengo claro que recopilaron toda la información de Roger Dingledine, que me compró un billete de avión por un tema de trabajo: su tarjeta de crédito, la dirección de compra, el navegador que usó y cualquier información relacionada con el billete de marras.

JULIAN

¿Y todo eso fue a parar al gobierno estadounidense? ¿No se limitaron a almacenarlo en un procesador comercial?

JACOB

Exacto. Los datos comerciales fueron recopilados, enviados al gobierno y posteriormente contrastados unos con otros. Y lo que a mí me alucina es que es precisamente de la fusión de estas tres cosas de lo que estabas hablando aquí. De mi derecho a viajar libremente, de mi capacidad para comprar un billete de avión o de que un tercero lo compre por mí, y de mi capacidad para poder expresarme de manera eficaz —viajaba para dar una charla en algún sitio, y para hacerlo tuve que asumir compromisos en otras dos esferas. Y, de hecho, eso afecta a mi capacidad de expresión, sobre

todo cuando me doy cuenta de la información que han recopilado y de los cabos que han atado.

Censura

JULIAN

Jake, ¿nos puedes contar algo acerca de tu detención en los aeropuertos de Estados Unidos y sobre cuáles fueron los motivos?

JACOB

Ellos afirmaron que me detenían porque: «Yo sé por qué».

JULIAN

Pero ¿no te lo dicen?

ANDY

Voy a intentar resumirlo, porque la seguridad técnica y la seguridad interna del Estado son dos cosas totalmente diferentes. Puedes tener un sistema totalmente seguro y el

gobierno pensará que no es bueno, pues para ellos, seguro es todo aquello que ellos puedan investigar, que puedan controlar, todo sistema en el que puedan irrumpir violando su seguridad técnica. El problema no era que Jake cogiera un vuelo para matar a alguien, secuestrar el avión o ese tipo de cosas. El problema radica en la capacidad que Jake tenía de comprometer ciertos asuntos gubernamentales al viajar a otros países, hablar con otra gente, y difundir sus ideas. Eso es lo más peligroso que existe actualmente para los gobiernos —que la gente tenga mejores ideas que sus políticas.

JACOB

Te agradezco el cumplido que me haces con tu afirmación, pero me gustaría puntualizar que la historia es todavía peor, porque ellos recopilan esta misma información de todo el mundo. Esto me pasó antes de que hiciera nada digno de mención; se debió exclusivamente a que estaba de viaje y los propios sistemas, la arquitectura, fomentaban esta recopilación de datos. Esto sucedió antes de que me detuvieran por cualquier cosa, fue antes de que me deportaran del Líbano, antes de que el gobierno estadounidense se interesara por mí.

ANDY

Tal vez lo previeran, tal vez lo vieron antes que tú.

JACOB

Por supuesto que lo hicieron, en parte gracias a la información que habían recopilado. Sin embargo, cada vez me daban una respuesta diferente. Lo que sí me decían siempre, sin excepción, era: «Porque podemos». Y yo decía: «De acuerdo, no discuto vuestra autoridad —mejor dicho sí la discuto, pero no ahora— sólo quiero saber por qué me está pasando esto a mí». Ahora la gente no para de decirme: «Bueno ¿no es evidente? Trabajas en Tor» o «Estás sentado al lado de Julian ¿qué esperabas?». Lo más alucinante es que cada una de las personas que me retuvieron —casi todas del Servicio de Aduanas y Protección Fronteriza y de la Oficina de Inmigración y Aduanas de Estados Unidos— me decía que lo hacía sobre todo porque tenía la autoridad para hacerlo. También me han dicho estupideces como: «Oh, ¿te acuerdas del 11 de septiembre? Por eso» o «Porque queremos que respondas a algunas preguntas y éste es el lugar donde tienes menos derechos, te lo aseguramos».

Y en una situación como ésa te deniegan el acceso a un abogado, te deniegan el acceso al cuarto de baño, pero te dan agua, te dan algo para beber, algo diurético, a fin de convencerte de que realmente quieres cooperar de alguna manera. Hicieron esto para presionarme, por razones políticas. Me preguntaron qué me parecía la guerra de Irak, qué opinaba de la guerra afgana. Básicamente, en cada paso

que daban repetían las tácticas del FBI durante el programa de contrainteligencia COINTELPRO (el programa de operaciones encubiertas aplicado entre los años 1956 y 1971). Por ejemplo, intentaron imponer su autoridad para cambiar realidades políticas de mi propia vida, y me presionaron no sólo para que las cambiara sino para que les diera acceso a todo aquello que me rondaba en la cabeza. También han confiscado mis bienes. En realidad no tengo libertad para hablar de todas las cosas que me ocurrieron porque es entrar en un terreno muy turbio, y ni siquiera sé si me está permitido hablar de ello. Estoy seguro de que esto le ha pasado a otras personas, pero lo cierto es que nunca he oído a nadie que lo cuente.

Una vez estaba yo en el aeropuerto Pearson de Toronto, y me disponía a volver a casa tras un evento familiar. Viajaba a Seattle, ciudad donde vivía en aquel entonces, y me detuvieron, me sometieron a una segunda inspección y a una tercera, y luego me metieron en un calabozo. Y me retuvieron tanto tiempo que cuando finalmente fui liberado perdí el vuelo. Pero lo curioso es que estas áreas de detención preventiva en realidad son técnicamente suelo estadounidense en suelo canadiense, así que tienen una norma que dice que si pierdes el vuelo o si falta mucho para el siguiente, te tienes que marchar. Así que técnicamente fui expulsado de América por estar detenido tanto tiempo y tuve que entrar de nuevo en Canadá, volar por todo el país,

alquilar un coche y luego conducir hasta la frontera. Y cuando llego a la frontera, me preguntan: «¿Cuánto tiempo ha estado usted en Canadá?» Y yo les digo: «Bueno, cinco horas más el tiempo que he estado detenido en Toronto». De modo que llevaba en Canadá unas ocho horas, y ellos me dicen: «Bien, entre, vamos a detenerle de nuevo». Desmontaron mi coche, me cogieron el ordenador e inspeccionaron todo lo que tenía, y luego me detuvieron. Me dejaron ir al cuarto de baño tras media hora, digamos que fueron de lo más compasivos. Y esto es lo que ellos llaman «excepción de búsqueda en las fronteras». Este tipo de actuaciones se produce porque ellos tienen la capacidad, aseveran, de hacerlo, y nadie cuestiona su actuación.[1]

JULIAN

Y esto es lo que te ha pasado a ti, pero los chinos con los que tengo relación, cuando me hablan del gran cortafuegos de China —en Occidente hablamos de ello en términos de censura: el bloqueo que sufren los ciudadanos chinos para salir del país o poder leer lo que opinan sobre el gobierno chino en Occidente y los disidentes chinos y el Falung Gong, y la BBC, y, para ser justos, también la propaganda china—, reconocen que su verdadera preocupación no es la censura propiamente dicha. Lo que verdaderamente les preocupa es que para que haya censura en internet necesitan vigilancia de internet. Para saber lo que

busca cada uno, para saber si está permitido o no, tienes que estar viéndolo, y si lo estás viendo eso significa que lo puedes grabar. Y esto tiene un tremendo efecto paralizador entre los chinos, no el hecho de que sean censurados sino que todo aquello que leen está siendo espiado y registrado. En realidad, eso es lo que nos está sucediendo a todos. Esto es algo que cambia a las personas cuando toman conciencia de ello. Cambia su comportamiento, cada vez menos combativo con respecto a los distintos tipos de autoridad.

JACOB

Sin embargo, esa es la respuesta equivocada a este tipo de influencia. El acoso que sufrí en la frontera no es un hecho aislado, todo árabe-americano, desde el 11 de septiembre y antes, ha tenido que enfrentarse a este tipo de acciones. La diferencia es que yo me niego a que la ventaja de ser blanco y tener pasaporte estadounidense se quede en agua de borrajas, y me niego a callarme porque lo que están haciendo está mal y porque están cometiendo un flagrante abuso de poder. Y nosotros debemos alzarnos en contra de este tipo de abusos, como se alzan en China voces valientes como la de Isaac Mao.[2] Isaac lleva años combatiendo activamente este tipo de censura, porque la respuesta no está en resignarse a este tipo de presión por el mero hecho de que el gobierno se declare competente para ejercerla.

JÉRÉMIE

Pero una vez más estamos hablando de política, porque lo que dices es, básicamente, que la gente debería combatir por sus derechos; sin embargo, antes la gente debe entender por qué debe combatir y, para hacerlo, debe tener la posibilidad de comunicarse. Yo tuve ocasión de entrevistarme con varios chinos —no sé si tenían algún cargo estatal o si fueron elegidos a dedo para salir y hablar conmigo—, y cuando les hablaba de la censura de internet a menudo me daban la siguiente respuesta: «Bueno, es por el bien de la gente. Hay censura, sí, porque si no existiera, habría comportamientos extremistas, existirían cosas que a todos nos disgustarían, y por eso el gobierno toma este tipo de medidas, para asegurarse de que todo vaya bien».

JACOB

Ese es el mismo argumento que el que se aplica a la extracción de órganos. ¡No desperdiciemos esos órganos!

JÉRÉMIE

Si te fijas en cómo se está llevando a cabo la censura china, verás que desde el punto de vista técnico cuenta con uno de los sistemas más avanzados del mundo.

JACOB

Absolutamente cierto.

JÉRÉMIE

Y me han dicho que en Weibo —el Twitter chino— el gobierno puede filtrar algunos *hashtags* o palabras clave para asegurarse de que no abandona ninguna de las provincias seleccionadas.

JACOB

Es clave recordar que cuando la gente habla de censura en Asia siempre hacen referencia a «los otros», como si sólo afectara al «vecino de al lado». Es importante recalcar que cuando buscas en Google en Estados Unidos, te dicen que han omitido ciertos resultados de búsqueda por motivos legales. Hay una diferencia entre ambos sistemas —en cómo se implementan, y, por supuesto, en la realidad social del cómo, el porqué e incluso el dónde—, pero gran parte de eso responde a la arquitectura. Por ejemplo, en la internet americana la arquitectura está muy descentralizada, sería francamente complicado aplicar el estilo de censura chino.

JULIAN

Bueno, un gran pedazo es Google, y a Google se le puede censurar. Hay cientos de páginas que mencionan WikiLeaks censuradas por Google.

JACOB

Sí, sin duda. Y, de hecho, desde el propio índice se puede hacer un análisis diferencial.

JULIAN

Sí, en teoría.

JACOB

En teoría. Y en la práctica, porque también hay gente que actualmente está trabajando en ese tipo de detección de censura, y lo hace analizando las diferencias que existen entre las distintas perspectivas de censura que se aplican en el mundo. Creo que es importante recordar que la censura y la vigilancia no son asuntos «de otros lugares». A la gente de Occidente le encanta decir: «Los iraníes y los chinos y los norcoreanos necesitan anonimato y libertad, pero a nosotros aquí no nos hacen falta». Y por «aquí», normalmente quieren decir «en Estados Unidos». Sin embargo no es sólo un tema de regímenes opresivos, pues si perteneces a las altas esferas de este tipo de regímenes el sistema no será opresivo contigo. No obstante, todos consideramos al Reino Unido como un lugar maravilloso; por lo general la gente cree que Suecia es un lugar bastante agradable, y sin embargo, a la vista está que cuando pierdes el favor de aquellos que detentan el poder, no acabas en una posición muy prometedora. Sin embargo Julian sigue vivo ¿no? Así que eso es un signo evidente de que estamos en

un país libre ¿no es cierto?

JULIAN

Trabajo duro para mantener mi posición actual. Pero tal vez deberíamos hablar sobre la censura de internet en Occidente. Es muy interesante. Si nos remontamos al año 1953 y echamos un vistazo a la *Gran enciclopedia soviética*, que se distribuía en todas partes, ésta incluía en ocasiones ciertas rectificaciones que informaban de los cambios que acontecían en la política de la Unión Soviética. En 1953, Beria, el jefe del NKVD, la policía secreta soviética, murió y perdió el respaldo político, de modo que el apartado que le describía con grandes elogios fue eliminado por los directivos de la enciclopedia y sustituido por una rectificación que debía «pegarse» en todos los volúmenes. Era extremadamente obvio. Menciono este ejemplo porque fue tan evidente y tan detectable que el intento pasó a formar parte de la historia. Mientras que en Reino Unido tenemos al diario *The Guardian*, y otros importantes periódicos sacando historias de los archivos de internet subrepticiamente, sin ningún tipo de descripción. Si intentas buscar esas páginas ahora, historias como el fraude del multimillonario Nadhmi Auchi, te encuentras sistemáticamente con lo siguiente: «Página no encontrada», porque también la han eliminado de los índices.

Permitidme que os cuente mi participación en el caso de

Nadhmi Auchi. En el año 1990 Irak invadió Kuwait, y eso desembocó en la primera guerra del Golfo. El gobierno kuwaití en el exilio, y también a la vuelta de éste, necesitaba efectivo, así que empezó a vender una serie de activos que incluían, entre otros, varias refinerías de petróleo fuera de Kuwait. Un empresario británico, Nadhmi Auchi, que había emigrado a Reino Unido a principios de los años ochenta desde Irak, en donde había sido una figura importante bajo el régimen de Saddam Hussein, actuó de intermediario en ese negocio. A consecuencia de esta intermediación fue acusado de participar en la canalización de 118 millones de dólares en concepto de comisiones ilegales. Fue la mayor investigación de un caso de corrupción en la historia de la Europa de postguerra. En el año 2003, Auchi fue acusado de fraude en lo que se conocería como el escándalo Elf-Aquitane. No obstante, a día de hoy tiene más de 200 empresas domiciliadas en su holding de Luxemburgo, y otras tantas en Panamá. Actualmente participa en los contratos de telefonía móvil firmados tras la guerra de Irak y en muchos otros negocios alrededor del mundo.[3]

En Estados Unidos, Tony Rezko, recaudador de fondos en la campaña para el Senado de Barack Obama, fue durante mucho tiempo colega de Auchi, quien a su vez había sido su principal financiador. Asimismo, ambos se vieron envueltos en la trama que apuntaba al antiguo gobernador de Illinois, Rod Blagojevich. Tanto Rezko como Blagojevich fueron

acusados de corrupción, Rezko en el año 2008 y Blagojevich entre finales del año 2010 y principios del 2011 (tras la interceptación por parte del FBI de una llamada telefónica intentando vender el antiguo escaño de Obama en el Senado). En el año 2007/2008, cuando Obama iniciaba su carrera como candidato presidencial de los demócratas, la prensa estadounidense empezó a investigar las conexiones de Obama. Investigaron a Rezko y revelaron la existencia de ciertos vínculos en relación con la compra de la casa de Barack Obama. En el año 2008, poco antes del juicio, Rezko recibió una transferencia de Auchi por importe de tres millones y medio de dólares de la que no informó al tribunal pese a los requerimientos de este último, razón por la cual fue encarcelado. De modo que el escrutinio de la prensa se centró en Auchi, quien, en aquella época instruía a los abogados británicos Carter-Ruck para iniciar una enérgica campaña en contra del reportaje publicado en el año 2003 sobre el escándalo Elf-Aquitaine y su condena en Francia. La campaña fue un éxito. Demandó a la prensa británica e incluso a blogs estadounidenses y, por lo que sabemos, consiguió que se eliminaran alrededor de una docena de artículos. La mayoría de estos artículos, incluidos los archivos de los diarios británicos, simplemente desaparecieron. Era como si nunca hubieran existido. No hubo ningún tipo de: «Hemos recibido una demanda legal y por este motivo hemos decidido retirar la historia». También

desaparecieron de los índices. WikiLeaks los desenterró y los republicó.[4]

JACOB

La historia del borrador.

JULIAN

La historia no sólo se modifica, sino que es como si nunca hubiera existido. Es la máxima de Orwell: «Quien controla el presente controla el pasado y quien controla el pasado controla el futuro.» Es la indetectable supresión de la historia en Occidente, y eso sólo tiene un nombre: censura postpublicación. La autocensura de la prepublicación es mucho más extrema y, a menudo, difícil de detectar. Lo hemos visto con los documentos del *Cablegate,* pues WikiLeaks trabaja con socios de distintos medios internacionales de comunicación, y eso nos permite ver cuáles censuran nuestro material y cuáles no.[5]

Por ejemplo, *The New York Times* censuró un cable que decía que millones de dólares habían sido distribuidos para influenciar de manera encubierta a ciudadanos libios con contactos políticos a través de compañías petrolíferas que operaban en Libia. El cable ni siquiera mencionaba un nombre o una empresa concreta, *The New York Times* simplemente redactó la frase siguiente: «Compañías de servicios petrolíferos.»[6] Probablemente lo más flagrante

fue el uso por parte de *The New York Times* del cable de la página número 62 sobre el programa norcoreano de misiles, donde se planteaba la posibilidad de que hubieran vendido misiles a los iraníes, y del que *The New York Times* usó dos párrafos para argumentar, en relación con ese asunto, que Irán disponía de misiles que podían alcanzar a Europa, pese a que más adelante en ese mismo cable se argumentaba precisamente todo lo contrario.[7]

El diario *The Guardian* clasificó un cable sobre Yulia Tymoshenko, ex primera ministra de Ucrania, en el que se planteaba la posibilidad de que estuviera escondiendo su patrimonio en Londres.[8] Censuró todos los comentarios que apuntaban a la corrupción generalizada de la élite Kazaja, sin mencionar siquiera un nombre, y también las notas que denunciaban que tanto ENI, la compañía italiana de energía que operaba en Kazajstán, como British Gas, eran empresas corruptas.[9]

The Guardian censuraba básicamente todos los ejemplos de los cables en los que una persona rica era acusada de algo, salvo en los casos en que el diario tuviera una agenda institucional en contra de la persona en cuestión.[10] A tal punto llegaba que, por citar un ejemplo, en un cable sobre el crimen organizado búlgaro se mencionaba a un ciudadano ruso, y *The Guardian* presentó la noticia como si todo girara en torno a él, como si él fuera el único culpable, haciendo caso omiso de la larga lista de

organizaciones e individuos vinculados con el crimen organizado búlgaro.[11] El diario alemán *Der Spiegel* censuró un párrafo en el que se decía que lo que estaba haciendo Merkel no respondía en absoluto a razones humanitarias, sino puramente políticas.[12] Hay muchísimos ejemplos.[13]

ANDY

Nuestra comprensión de la libertad de información y de la libre circulación de la información es en cierto sentido un concepto muy nuevo y radical si observamos el planeta Tierra. Diría que no hay grandes diferencias entre Europa y otros países. Bueno, los hay que tienen un marco democrático, lo cual significa que podemos leer y entender, y puede que incluso combatir legalmente la infraestructura de la censura, pero eso no significa que no exista, mientras que en países como Arabia Saudí o China combatirla nos costaría bastante más.

JULIAN

Mi experiencia es que Occidente es mucho más sofisticado en cuanto al número de capas de falsedad y ofuscación que esconden lo que realmente está ocurriendo. La función de estas capas consiste en negar la censura que impera en nuestros días. La censura es como una pirámide. En dicha pirámide sólo la cúspide sobresale de la arena, y

eso está hecho adrede. La cúspide es pública —demandas por difamación, asesinatos de periodistas, cámaras que son confiscadas por el ejército...—, censura públicamente declarada. Sin embargo ésa es una parte ínfima. Bajo la cúspide, tenemos la siguiente capa, conformada por todos aquellos que no quieren estar en la cúspide, aquellos que aplican la autocensura para no acabar allí. La tercera capa comprende todas las formas de incentivo económico o trato de favor que se dispensa a ciertas personas para que escriban sobre esto o aquello. La cuarta capa es la de la economía pura y dura: aquello sobre lo que es rentable escribir, aun en el caso de que no incluyas los factores económicos que conforman la cúspide de la pirámide. La siguiente capa está hecha del prejuicio de los lectores que cuentan con un nivel limitado de educación, ya que, por un lado, se les puede manipular fácilmente con información falsa y, por otro, habida cuenta de sus limitaciones, ni siquiera puedes plantearles verdades sofisticadas o complejas. La última capa es la de la distribución, que se traduce en que algunas personas, por ejemplo, no pueden acceder a la información en un idioma determinado. Y así opera la pirámide de la censura. Lo que *The Guardian* está haciendo al clasificar los documentos del *Cablegate* responde a la definición de la segunda capa.

No obstante, por lo general se tiende a negar la existencia de este tipo de censura, bien porque no sale a la

luz o porque no hay instrucciones concretas para censurar determinados asuntos. Los periodistas rara vez reciben instrucciones del tipo: «No publiques nada sobre tal tema» o «No publiques tal suceso». Más bien son ellos mismos los que dan por hecho que deben hacerlo, porque comprenden los intereses de aquellos a quienes desean apaciguar o cuya amistad les interesa. Si te portas bien recibirás una palmadita en la espalda y tu compensación; de lo contrario, no percibirás nada. Es así de simple. Para ilustrarlo siempre me ha gustado utilizar el siguiente ejemplo: la censura palmaria que tuvo lugar en la Unión Soviética, la censura a la que tanto bombo se dio en Occidente —militares asaltan los hogares de los periodistas en mitad de la noche para llevárselos presos—, sólo ha sufrido un ligero cambio horario de doce horas. Ahora esperamos a la luz del día para tomar los hogares de aquellos periodistas que pierden el favor de sus «mecenas» y no pueden saldar sus deudas. Los periodistas son expulsados de sus casas porque se las han embargado. Las sociedades occidentales son especialistas en blanquear la censura y en estructurar los asuntos de los poderosos de manera que cualquier discurso público que logre abrirse camino afronte grandes dificultades para poder hacer mella en las verdaderas relaciones de poder de una sociedad altamente fiscalizada, pues dichas relaciones se esconden en las capas de la complejidad y el secretismo.

ANDY

Jérémie mencionó a los pedo-nazis.

JACOB

Volvemos a los pedo-nazis…

JÉRÉMIE

Dos jinetes en uno.

ANDY

Los pedo-nazis resumen bastante bien los argumentos de censura alemanes e incluso puede que también una parte de los argumentos europeos. Alemania no quería ningún tipo de contenido xenófobo en internet debido a su historia y, evidentemente, si tú le dices a la gente que necesitas limitar internet a causa de los pedófilos entonces tienes vía libre para hacer cualquier cosa. Además, había un documento interno de trabajo de la Comisión Europea sobre retención de datos que proponía lo siguiente: «Deberíamos hablar más sobre pornografía infantil, de esta manera conseguiremos que la gente se muestre a favor».[14]

JULIAN

¿Puedes explicarte un poco más? Lo que dices es que si nosotros censuramos una sola cosa, pongamos por caso la

pornografía infantil, entonces para evitar que la gente vea pornografía infantil necesitamos vigilar todas y cada una de las cosas que la gente hace. Necesitamos construir esa infraestructura. Necesitamos construir un sistema de espionaje y censura masivos para una sola cosa.

ANDY

Está en el detalle de la mecánica —el llamado sistema de precensura en Alemania te obliga a nombrar a la persona legalmente responsable de aquello que publicas. De modo que, por así decirlo, si publicas algo, ya sea en un trozo de papel o en internet, sin especificar quién es legalmente responsable del contenido, técnicamente estás violando la ley. Esto significa que tú puedes asignar la responsabilidad y si alguien viola la ley al distribuir, pongamos por caso, pornografía infantil o discursos xenófobos, podrías simplemente decir: «De acuerdo, veamos dónde está ubicado ese tío, le atrapamos y eliminamos el material de la red».

JULIAN

Eso significa que censuramos al editor en lugar de censurar al lector.

ANDY

Sí. Y esto es vigilar cosas concretas. Podría estar de acuerdo en que no todo necesita estar disponible a todas

horas, porque si miro discursos xenófobos a veces aparecen cosas con direcciones privadas de personas y demás que pueden llevarnos a situaciones que no me gustan.

JULIAN

Pero Andy, eso que dices es muy alemán. Para hacer eso, para determinar qué va a ser aceptable y qué no, tienes que tener un comité, tienes que nombrar a los miembros de ese comité, tienes que tener un proceso de nombramientos...

ANDY

Sí, tenemos toda esa mierda. Los asesinatos en la segunda guerra mundial, todo lo que los nazis hicieron, todas las propiedades que confiscaron... Te daban un recibo, hacían una lista. Todo era burocracia. Puedes decir que los alemanes mataron injustificadamente a muchísima gente —es cierto—, pero lo hicieron de una manera burocrática. Eso es Alemania.

JULIAN

Si tuvieras a alguien decidiendo qué debería censurarse y qué no, entonces necesitarías dos cosas. En primer lugar, tienes que construir una arquitectura técnica para aplicar la censura. Tienes que construir una maquinaria de censura a escala nacional para poder hacerlo de una manera eficaz. Y en segundo lugar, necesitas una burocracia y un comité

encargado de censurar. El comité debe ser en esencia secreto, porque es completamente inútil a menos que sea secreto, y al final lo que tienes es una justicia secreta.

ANDY

¿Sabes una cosa? En Alemania tenemos un buen principio.

JACOB

¿Sólo uno?

ANDY

El principio es que si es tan poco realista como aplicar una ley, entonces no debería estar ahí. Si una ley no tiene sentido, como por ejemplo prohibir los molinos de viento, entonces decimos: «¡Eh, vamos, olvídalo!». A los que estamos aquí nos inspira la internet que conocimos en sus inicios, la libre circulación de información, entendiendo por libre: ilimitada, sin bloqueos, sin censuras, sin filtros. De modo que si aplicamos nuestra idea de libre circulación de información al planeta Tierra —y de hecho se ha aplicado en términos generales a todo el planeta— vemos, sin duda, hasta qué punto ha afectado a gobiernos y cómo estos han aplicado su poder, y la manera en que han orquestado la censura, ya sea precensura, postcensura, o cualquier otro tipo de censura. Todos conocemos los intrincados

conflictos que han surgido después. La cuestión es saber cuál es nuestra idea de gobierno o de una hipotética organización postgubernamental —tal vez WikiLeaks sea la primera organización de este tipo—, porque no tengo claro que los gobiernos sean la respuesta a todos los problemas de este planeta, como los medioambientales, por ejemplo.

JULIAN

Los gobiernos tampoco tienen claro dónde está la frontera entre lo que es gobierno y lo que no. Hoy los límites están completamente distorsionados. Los gobiernos ocupan espacio, pero WikiLeaks ocupa parte del espacio de internet. El espacio de internet está incrustado en el espacio real, pero el grado de complejidad que existe entre el objeto incrustado y el incrustador hace que al incrustador le cueste incluso reconocer que el objeto incrustado forma parte de él. Por eso tenemos esta sensación de que un ciberespacio —como una suerte de reino que, de hecho, existe en alguna parte—, lo es por su nivel de oblicuidad, complejidad y universalidad. Cuando lees algún archivo en internet alojado en una ubicación es como si lo leyeras en cualquier otra, o en el futuro, ésa es su universalidad. De modo que en ese sentido, como organización que ocupa el ciberespacio, y como experta en mover su información a través de las incrustaciones subyacentes, tal vez seamos una organización postestatal, precisamente debido a esa falta de

control geográfico.

No quiero llevar esta analogía demasiado lejos porque estoy bajo arresto domiciliario. La fuerza coercitiva de los Estados obviamente es extensiva a toda nuestra gente, allí donde se sabe quiénes son. Pero al resto de la prensa le gusta decir que somos una agencia de comunicación sin Estado, y aciertan al calificarnos de apátridas. Yo solía decir: «Bueno ¿Qué crees que es Newscorp? Es una gran multinacional». Sin embargo, Newscorp está estructurada de tal manera que puedes conseguir sus componentes clave, y ésa es la razón por la que tiene tantos problemas aquí en Reino Unido con el escándalo del hackeo de teléfonos, y por eso intenta por todos los medios hacer la pelota al sistema estadounidense. No obstante, si los activos de una organización son fundamentalmente su información, entonces puede ser transnacional de una manera difícilmente evitable gracias a la criptografía. Esto explica el bloqueo económico que se nos ha impuesto —otras facetas de nuestra organización son más difíciles de reprimir.[15]

JACOB

Estamos hablando de esto en términos utópicos, tenemos que volver atrás. Me preguntaste antes sobre el acoso al que fui sometido, me has preguntado sobre la censura en Occidente y te he hablado del programa de asesinatos selectivos de Obama, que ellos consideran legal

porque hay un proceso y, por consiguiente, se considera un proceso justo.

JULIAN

Un proceso secreto diría yo.

JACOB

Esto tiene mucho que ver con caso de John Gilmore. Una de las demandas que interpuso John Gilmore apelando a su derecho a viajar anónimamente en el interior de Estados Unidos se topó con un tribunal que le dijo literalmente: «Mira, vamos a consultar la ley, que es secreta. La leeremos y averiguaremos si esta ley secreta también te permite hacer eso que, por ley, te está permitido hacer». Y cuando leyeron la ley secreta se encontraron con que, de hecho, le estaba permitido viajar sin identificación, porque lo que la ley secreta no coartaba era su derecho. Él nunca tuvo la menor idea de lo que era aquella ley, pero el hecho es que, posteriormente, en respuesta a la sentencia en favor de Gilmore, se modificaron las políticas de la Administración de Seguridad en el Transporte (Transportation Security Administration, TSA) y del Departamento de Seguridad Nacional de Estados Unidos, pues al final resultó que la ley secreta no era lo suficientemente restrictiva en este sentido. [16]

JULIAN

Entonces ¿las hicieron más restrictivas?

JACOB

En efecto, a través de leyes habilitantes. Pero es importante recalcar que el programa de asesinatos selectivos, el acoso que la gente sufre en las aduanas, la censura que encontramos en la red, la censura que las compañías llevan a cabo a instancias de un gobierno o de una corporación, todas estas cosas tienen un nexo común. Y en realidad todo se reduce a que el Estado tiene demasiado poder en todos y cada uno de los lugares en que observamos este tipo de acciones. Esto se debe a que el poder se ha concentrado en estas áreas y ha atraído a personas que abusan de él, o que presionan para que se ejerza. Y aunque en ocasiones hay casos legítimos, lo que vemos es que el mundo estaría muchísimo mejor si no existiera esa centralización, si no existiera la tendencia hacia el autoritarismo.

Occidente no es una excepción en este tema, porque al fin y al cabo si ahora tenemos un «zar» de la ciberseguridad, en fin, eso no difiere gran cosa de los «zares» que dirigían las fuerzas de seguridad interna de cualquier nación hace medio siglo. Estamos construyendo el mismo tipo de estructuras de control autoritario, estructuras que inevitablemente atraerán a personas que abusarán de ellas, y

eso es algo que en Occidente todos tratamos de simular que es diferente. Pero no lo es. Porque en Occidente existe una línea continúa de gobierno que va del autoritarismo al liberalismo libertario. No lo digo en el sentido americano de partido político, sino en este sentido: en el de la continuidad. Estados Unidos está muy lejos de la Unión Soviética en muchísimos aspectos pero, con todo, ambos países están mucho más cerca el uno del otro que de Christiania, el barrio independiente en el corazón de Copenhague, en Dinamarca. [17] Y está todavía más lejos, creo, del hipotético mundo ideal que podría existir si construyéramos una flamante colonia en Marte. Trataríamos por todos los medios de que, sea lo que fuere aquello que construyéramos en Marte, estuviese lo más lejos posible del totalitarismo y del autoritarismo. Si eso no es posible, algo falla.

JÉRÉMIE

De nuevo todos esos temas están unidos. Cuando hablamos de poder concentrador estamos hablando una vez más de arquitectura. Y cuando hablamos de censura de internet estamos hablando de centralizar el poder para determinar los contenidos a los que la gente puede o no acceder, y de si la censura gubernamental o incluso la privada constituye un poder excesivo. Nosotros tenemos el ejemplo siguiente: nuestra página web laquadrature.net fue censurada en el Reino Unido por Orange UK durante varias

semanas. Estaba en la lista de sitios web que Orange vetó a los menores de dieciocho años. Tal vez mencionamos el término pornografía infantil cuando nos opusimos a ese tipo de legislación, o puede que simplemente no les gustáramos porque también nos habíamos opuesto a su política en contra de la neutralidad de la red al abogar por una ley que les prohibiera discriminar las comunicaciones de sus usuarios.[18] Nunca lo sabremos. Pero lo cierto es que aquí tenemos actor privado que, como servicio, proponía quitar a la gente la capacidad de acceso a la información en internet. Creo que esto comporta un importante riesgo, más allá del poder que otorguemos a Orange, al gobierno de China o a quien sea.

JACOB

Aclaración: cuando dices privado en el Reino Unido ¿quieres decir que ellos son los únicos dueños de todas las líneas, de las conexiones de fibra y de todo lo demás, o utilizan algunos de los recursos del Estado? ¿Cómo se concedían las licencias de ondas de radio? ¿No participaba el Estado en ningún sentido? ¿No tienen el deber de diligencia?

JÉRÉMIE

Las concesiones existen. Tanto el gobierno como la empresa privada están cambiando la arquitectura de internet,

que pasa de ser una red universal a convertirse en balcanización de pequeñas subredes. Pero lo que aquí estamos discutiendo desde el principio son asuntos de carácter global, ya hablemos de la debacle del sistema financiero, o de la corrupción; ya hablemos de geopolítica, de energía, o de medioambiente. Todos ellos son problemas globales a los que la humanidad se enfrenta a día de hoy, y todavía contamos con una herramienta global que permite una mejor comunicación, un mejor intercambio de conocimiento, una mejor participación en los procesos políticos y democráticos. Sospecho que una internet global y universal es la única herramienta que tenemos para resolver esos problemas globales, y eso explica por qué esta batalla por una internet libre es la principal batalla que todos debemos librar aquí.

ANDY

Estoy totalmente de acuerdo en que necesitamos asegurarnos de que internet se conciba como una red universal con libre circulación de información; en que necesitamos no sólo definir esto muy bien, sino también identificar a aquellas compañías y a aquellos proveedores de servicios que ofrecen algo que ellos llaman internet, pero que es en realidad otra cosa completamente diferente. Sin embargo, creo que no hemos respondido a la cuestión clave que esconde el asunto de los filtros. Quiero poneros un

ejemplo que ilustra lo que yo creo que debemos responder. Hace años, unos diez años, nosotros nos declaramos en contra de que Siemens suministrara el llamado software de filtro inteligente. Siemens es una de las mayores empresas de telecomunicaciones de Alemania y una importante proveedora de inteligencia. El caso es que Siemens se dedicaba a vender este sistema de filtrado a empresas a fin de que, por ejemplo, los empleados no pudieran acceder al sitio de los sindicatos para informarse sobre sus derechos laborales y demás. Y también bloquearon el sitio web del Club del Caos Informático, cosa que nos dejó totalmente decepcionados. Tildaron su contenido de «delictivo» o algo parecido, por lo que nosotros emprendimos acciones legales. Y en una feria decidimos organizar un enorme encuentro de protesta y rodear los stands de Siemens e «interceptar» a la gente que entraba y salía. Lo curioso fue que lo anunciamos en nuestro sito web con la intención de atraer al mayor número de personas posible a través de la red, y la gente del stand de Siemens no tenía ni la menor idea porque también ellos utilizaban software de filtrado, de modo que ni siquiera pudieron leer un aviso que evidentemente estaba ahí.

JULIAN

El Pentágono estableció un sistema de filtrado mediante el cual se filtraba cualquier correo electrónico enviado al

Pentágono con la palabra WikiLeaks. Así que en el caso de Bradley Manning, la fiscalía, en su intento de enjuiciar el caso, por supuesto, escribió a personas ajenas al ejército sobre «WikiLeaks», pero nunca obtuvieron respuesta pues todas contenían la palabra «WikiLeaks».[19] La seguridad nacional del Estado puede que acabe devorándose a sí misma.

ANDY

Lo cual nos lleva de nuevo a una pregunta clave: ¿Existe la información que genera efectos negativos? Es decir, desde el punto de vista de la sociedad ¿queremos una internet censurada porque es mejor para la sociedad, o no? E, incluso en el caso de la pornografía infantil, podríamos alegar: «Espera un momento, la pornografía infantil pone de relieve la existencia de un problema, el abuso de niños, y para poder resolver el problema necesitamos conocerlo en profundidad».

JACOB

Lo que dices es que internet ofrece la prueba del delito.

JULIAN

Bueno, más bien diría que te proporciona un lobby.

ANDY

Ese sería un enfoque tremendamente radical, pero si hablamos de los nazis o ese tipo de cosas, hay que matizar un poco más. La gente que tiene familia se preguntará: «Bueno, ¿no es mejor para la sociedad filtrar las cosas malas para que podamos aferrarnos a las buenas, o significa eso limitar nuestra capacidad para ver los problemas y gestionarlos y afrontarlos y hacernos cargo de ellos?».

JÉRÉMIE

Creo que la solución no está en la censura. Cuando hablamos de pornografía infantil ni siquiera deberíamos utilizar la palabra pornografía, es más bien una representación de escenas delictivas de abuso infantil. Lo que habría que hacer es ir a los servidores e inutilizarlos, identificar a las personas que suben los contenidos para identificar a aquellas que los producen, es decir, a los que abusan de los niños en primera instancia. Y cuando haya una red de personas, una red comercial o de otro tipo, irrumpir en sus domicilios y arrestarlos. Ycuando aprobamos leyes —y en Francia tenemos una que establece que una autoridad administrativa del Ministerio del Interior es la responsable de decidir qué sitios web deben bloquearse—, estamos eliminando el incentivo de investigar servicios que nos permitan encontrar a las personas que cometen los delitos con el argumento de: «Oh, ya hemos vetado el acceso a las páginas de contenido malintencionado». Como

si poner la mano en el ojo de aquel que observa el problema significara realmente resolver el problema. De modo que, sólo desde esa perspectiva, cabría decir que todos coincidimos en lo siguiente: esas imágenes deberían ser eliminadas de internet.

JACOB

Lo siento, pero me dejas temblando. Es frustrante escuchar ese tipo de argumentos. Me dan ganas de vomitar, porque lo que acabas de hacer es lo mismo que decir: «Quiero utilizar mi posición de poder para imponer mi autoridad sobre los demás, quiero borrar la historia». Puede que sea un radical en este caso, y en otros muchos, no lo sé, pero me la voy a jugar. Eso que dices es un ejemplo más de que borrar la historia es un puro despropósito. Resulta que gracias a internet nos hemos enterado de que en la sociedad existe una epidemia que es el abuso infantil. Eso es lo que hemos aprendido del uso de la pornografía infantil —si bien debería llamarse explotación infantil—, tenemos pruebas de ello. Taparlo, borrarlo es, creo, un grave error, porque lo cierto es que podríamos aprender muchas cosas sobre la sociedad en sí misma. Por ejemplo puedes enterarte —y evidentemente nunca haré carrera en la política después de terminar esta frase— de quién la produce, y de las personas que son victimizadas. Es imposible que la gente haga caso omiso del problema. Lo cual significa que debemos empezar

a investigar la causa que lo origina, es decir los explotadores de niños. Irónicamente, ciertas tecnologías de vigilancia pueden ser útiles en el reconocimiento facial y en el análisis de los metadatos de las imágenes. Borrándolo, garantizando que vivimos en un mundo en el que se pueden eliminar ciertas cosas y otras no, creando esos cuerpos administrativos de censura y de vigilancia, nos encontramos en una pendiente resbaladiza que, como hemos visto, desemboca directamente en el problema de los derechos de autor y en el planteamiento de sistemas alternativos.

El hecho de que perseguir este tipo de acciones sea una causa noble no nos debería llevar por el camino fácil. Tal vez deberíamos intentar resolver los delitos, tal vez lo que deberíamos hacer es ayudar a aquellos que son victimizados, aunque ese tipo de ayuda comporte un coste. Tal vez, en lugar de hacer oídos sordos, deberíamos afrontar el hecho de que la sociedad tiene este gran problema y lo manifiesta en internet de una manera concreta.

Es por ejemplo como cuando Polaroid creó la cámara Swinger (la cámara instantánea de fotos) y la gente empezó a sacar fotos abusivas con dichas cámaras. La respuesta no está en destruir el medio, o en custodiar policialmente ese medio. Se trata de encontrar pruebas para perseguir los delitos que el medio ha documentado. La solución no consiste en debilitar el medio, no pasa por lisiar a la sociedad al completo por un asunto particular. Porque aquí hablamos

de pornografía infantil, pero hablemos de la policía. Es de dominio público que la policía abusa de la gente en muchos países. Es posible que existan muchos más abusos cometidos por policías en internet que por pornógrafos.

JULIAN

Lo que está claro es que hay más policías.

JACOB

Sabemos que hay un número «n» de policías en el mundo y sabemos que un número «x» de éstos han cometido violaciones éticas, normalmente violaciones graves. Basta observar el *Occupy movement* (movimiento de ocupación [inspirado en el 15-M]) para darnos cuenta de ello. Si censuramos, ¿debemos censurar internet porque sabemos que algunos polis son malos? ¿Debemos coartar la capacidad de la policía de hacer un buen trabajo policial?

JULIAN

Bueno, luego está el problema de la revictimización, que se produce cuando el niño, más adelante o cuando es adulto, o incluso sus allegados, ven de nuevo las imágenes del abuso.

JACOB

Mientras esos polis continúen en la red, yo estoy siendo revictimizado.

JULIAN

Sí, una imagen de ti siendo apaleado por un policía se puede considerar revictimización. Diría que la protección de la integridad de la historia de lo que realmente ha sucedido en nuestro mundo es más importante. A pesar de que la revictimización es una realidad, el hecho de establecer un régimen de censura capaz de eliminar grandes trozos de historia significa que nunca afrontaremos el problema, porque no podemos identificar el problema en sí. En la década de los noventa, yo asesoré en asuntos de internet a un cuerpo australiano de policías especializado en la lucha contra la pedofilia, la Victorian Child Explotation Unit. A aquellos policías no les gustaban los sistemas de filtrado, porque cuando la gente no puede ver que la pornografía infantil existe en internet, desaparece el lobby que garantiza que los policías dispongan de los fondos necesarios para frenar el abuso infantil.

JÉRÉMIE

El punto en el que todos coincidimos —creo que es el más importante— es que al final es una responsabilidad individual de las personas que hacen el contenido, el material de explotación infantil y ese tipo de cosas; eso es lo que realmente importa y en lo que los policías deberían trabajar.

JACOB

Nosotros no estamos de acuerdo. Yo no he dicho eso.

JULIAN

No, Jérémie habla de hacer, no de publicar. Hay una diferencia.

JACOB

La producción del contenido no es la cuestión. Os lo aclaro: si, por ejemplo, tú has abusado de un niño y Andy saca una foto de ello como prueba, no creo que Andy deba ser acusado.

JÉRÉMIE

No, me refiero a las personas que abusan. Vamos, hablo de los cómplices, de ayudar e instigar a la comisión de un delito.

ANDY

Sin embargo algunas personas abusan del niño para sacar fotos ¿no?

JACOB

Por supuesto que lo hacen.

ANDY

Puede que también haya un componente económico en este asunto.

JACOB

Estoy totalmente de acuerdo contigo. Estoy haciendo una distinción, y es para explicar que si el contenido es un registro histórico que prueba la comisión de un delito, evidencia la comisión de un delito muy grave, y si bien no deberíamos perder de vista el hecho de que hay revictimización, lo verdaderamente importante es la victimización original, existan o no fotos de la misma.

JÉRÉMIE

Por supuesto. A eso me refiero.

JACOB

Que existan fotos o no es prácticamente irrelevante. Cuando existen fotos, es importante recordar que hay que tener en cuenta la gratificación/recompensa, y ése es el gran objetivo para acabar con el daño y detener el abuso. Una gran parte del trabajo consiste en asegurarse de que haya pruebas y de que existan incentivos para que las personas que tengan las herramientas adecuadas puedan resolver este tipo de delitos. Eso, creo que es vital, y la gente suele perderlo de vista porque lo fácil es simular que nada existe, censurar los contenidos y luego decir que se ha erradicado

el abuso. Y no es cierto.

ANDY

Y el problema es que en este momento mucha gente se decantará por la solución fácil, porque a nadie le agrada ver lo que realmente está ocurriendo en la sociedad. Creo que vosotros sí tenéis una verdadera oportunidad de gestionar un problema político porque no estáis desarrollando una política que eluda el problema o lo haga invisible. Puede que en parte se trate de ciberpolítica, pero la verdadera cuestión está en cómo la sociedad afronta los problemas, y yo tengo serias dudas de que algo como la información cause directamente un perjuicio. El problema radica en la capacidad para filtrar, por supuesto, pero también es cierto que yo no quiero ver todas las fotos que internet pone a mi disposición. Hay algunas que me parecen verdaderamente repugnantes e inquietantes, pero lo mismo me pasa con las películas del videoclub de mi barrio. De modo que la pregunta es: ¿Tengo la capacidad para gestionar lo que veo, y lo que proceso, y lo que leo? Y ése es el enfoque adecuado de filtrado. A este respecto, Wau Holland, el fundador del Club del Caos Informático, hizo una divertida reflexión: «Ya sabes, las filtraciones deberían hacerse en el usuario final, y en el aparato final del usuario final».[20]

JULIAN

Entonces las filtraciones deberían hacerlas aquellos que reciben la información.

ANDY

Deberían hacerse aquí. Justo aquí [señalando a su cabeza].

JULIAN

En el cerebro.

ANDY

En el aparato final del usuario final, es decir, en esa cosa que tienes entre las orejas. Ahí es donde deberías filtrar tú, y no el gobierno en tu nombre. Si la gente no quiere ver las cosas, bueno, no tiene obligación, y, en los tiempos que corren, lo cierto es que hay muchas cosas que filtrar.

Privacidad para el débil, transparencia para el poderoso

JULIAN

Andy, hace poco hablé con el presidente de Túnez y le pregunté qué iba a pasar con los registros de inteligencia de la etapa del dictador Ben Ali —el equivalente en Túnez a los archivos de la Stasi— y me dijo que si bien éstos eran muy interesantes, las agencias de inteligencia eran un problema, que son peligrosas, y que tendría que acabar con todas ellas. Pero respecto a los archivos, pensaba que para la cohesión de la sociedad tunecina era mejor que siguieran manteniéndose en secreto para evitar que se iniciara un juego de acusaciones. Tú eras muy joven durante la caída de la Stasi en Alemania del Este, ¿nos puedes contar algo de los archivos de la Stasi? ¿Qué piensas del levantamiento del secreto de los archivos de seguridad?

ANDY

Probablemente Alemania cuenta con la agencia de inteligencia mejor documentada del planeta, o al menos con una de las mejores. Todos los documentos del Ministerio de la Seguridad del Estado de Alemania del Este (Stasi) —todos los cuadernos de notas, documentos procesales, documentos de formación, estudios internos—, son prácticamente públicos. Prácticamente significa que no todos son de fácil acceso, pero gran parte sí, y el gobierno ha creado una agencia encargada de los registros para que los ciudadanos alemanes puedan también ver aquellos archivos de la Stasi que les conciernen.

JULIAN

El gobierno alemán creó la comisión federal para la preservación de los archivos de la Stasi o BStU (Bundersbeaufragte für die Stasi-Unterlagen), esta enorme distribuidora de archivos de la Stasi.

ANDY

Sí, y los periodistas pueden efectuar las denominadas consultas de investigación, que bien podrían compararse con las solicitudes de libertad de información, para desarrollar sus estudios sobre el asunto. Y existen numerosos ensayos y también cuadernos de notas relacionados con el comportamiento estratégico de la Stasi. En verdad creo que es una buenísima cosa de la que

aprender. Entiendo que tal vez sea demasiado esperar que los tunecinos publiquen todos los archivos personales elaborados por la anterior agencia de inteligencia, pues el presidente —el presidente actual— se vería obligado a juzgar sus propios registros y los de sus acólitos. Estas agencias de inteligencia no respetan la privacidad, de modo que tendrán archivos personales sobre tu vida sexual, tus telecomunicaciones, tus transferencias bancarias, sobre cualquier cosa que hayas hecho que no desees revelar.

JULIAN

¿Seguiste el caso del Amn El Dawla en Egipto, el servicio interno de seguridad? Miles de personas irrumpieron en su sede, saquearon los archivos mientras el Amn El Dawla trataba de quemarlos y destruirlos y tirarlos a la basura, y gran parte del material salió a la luz. Podías comprar un archivo por dos dólares en cualquier mercado local y subirlo a la red. No ha destruido la sociedad egipcia.

ANDY

No, sólo digo que en parte entiendo que la gente no quiera que sus archivos personales salgan a la luz. Lo puedo entender, si viviera en un país que tuviera registrados cuarenta años de mi vida y que me grabara cada vez que voy al cuarto de baño...

JULIAN

¿Pero existe un análisis de coste-beneficio, no? Desde mi punto de vista, el que se convierte en rata, es rata para siempre.

ANDY

Exacto, pero el argumento ético del hacker es, básicamente, utilizar la información pública y proteger la información o los datos privados, y estoy convencido de que si defendemos la privacidad — y tenemos buenas razones para hacerlo— no deberíamos limitarnos a decir que las cosas están equilibradas a este respecto. Nosotros podemos distinguir. No es que tengamos que ponerlo todo en manos del público.

JACOB

Pero hay un beneficio asociado al secreto que es asistemático. Retrocedamos un momento. Tú partes de un argumento totalmente viciado, que es esta idea de que la información es privada cuando es limitada, y eso sencillamente no es verdad. Por ejemplo, en mi país, si todo el mundo tuviera una acreditación para acceder a información privada...

JULIAN

4,3 millones...

JACOB

¿Cómo puedes llamar privada a esa información? El problema es que en realidad no es ciento por ciento secreta para todos los habitantes del planeta.

JULIAN

Secretos del débil a disposición del poderoso.

ANDY

Sí, tienes razón. Pero si abriéramos el archivo del todo...

JULIAN

Ya se ha hecho en algunos países europeos.

ANDY

No. No conozco un solo país donde todos los registros hayan sido revelados.

JULIAN

En Polonia, por ejemplo, se sacaron a la luz más registros que en Alemania.

ANDY

Puede que sí. Lo que en realidad ocurrió, el lado oscuro del trato que ha hecho Alemania, es que utilizaron a antiguos oficiales de la seguridad del Estado de Alemania

Oriental para que la Stasi administrara no sólo sus propios registros, sino también los de la denominada «Nueva Alemania», la antigua parte oriental unificada. A este respecto hay una anécdota interesante sobre una empresa que ganó una licitación pública para limpiar el edificio donde se custodiaban los archivos. La empresa ganó el concurso sólo por ser la que ofertaba el precio más barato por el servicio objeto de licitación. Al cabo de seis años la organización que custodiaba los archivos descubrió que había contratado a una empresa constituida por antiguos oficiales de la inteligencia oriental con el fin de limpiar sus propios registros.

JÉRÉMIE

Había un informe sobre eso en WikiLeaks. Lo leí. Era genial.[1]

ANDY

WikiLeaks publicó el informe precisamente sobre eso, así que tienes razón al afirmar que cuando estos registros caen en manos de gente mal intencionada es complicado hablar de privacidad.

JULIAN

Sin embargo podemos extrapolarlo a un contexto más amplio. Internet nos ha llevado a una explosión de

información disponible para el público verdaderamente extraordinaria. La función educativa es extraordinaria. Por otro lado, la gente habla de WikiLeaks y dice: «Mira, toda esa información privada del gobierno es ahora pública, el gobierno no puede mantener nada en secreto». Y yo digo que eso es una soberana estupidez. Yo digo que WikiLeaks es la sombra de una sombra. En realidad, el hecho de que hayamos producido más de un millón de palabras de información y se la hayamos trasladado al público es fruto de la enorme explosión de material secreto que existe ahí fuera. Y, de hecho, los grupos de poder tienen tal cantidad de material secreto que la información que existe a disposición del público es una mínima parte, y las operaciones reveladas por WikiLeaks constituyen una pequeña fracción de este material de carácter privado. Cuando en un lado pones a los infiltrados poderosos, conocedores de todas las transacciones del mundo efectuadas con cualquier tarjeta de crédito, y en el otro al usuario-tipo de internet que busca información en Google, blogs y en los comentarios de otros usuarios, ¿cómo ves la balanza?

ANDY

Podría alegar que es bueno que todos estos registros salieran a la luz porque de ese modo todos sabrían que si utilizan sus tarjetas dejan un rastro. A alguna gente, si se lo

explicamos, le costará entender algo tan abstracto. Sin embargo en cuanto lean sus propios registros lo entenderán.

JULIAN

Basta con tu registro de Facebook, que tiene 800 megas de información sobre ti.

ANDY

Me consta que tras la caída del bloque comunista, el canciller alemán Helmut Kohl quería unificar Alemania y los americanos le pusieron una condición en el llamado tratado 2+4. Le dijeron que querían seguir manteniendo las telecomunicaciones alemanas bajo su control, bajo su vigilancia, y Kohl no le dio importancia porque no entendió lo que realmente es la vigilancia de las telecomunicaciones. Estuve con algunos miembros de su equipo y todos se mostraron disgustados con esta decisión, por lo que finalmente decidieron llevar a su despacho dos carritos con cerca de ocho mil páginas de transcripciones de sus llamadas telefónicas grabadas por la Stasi. Y él dijo: «¿Qué coño es eso?». Y ellos le respondieron: «Oh, son tus llamadas telefónicas de los últimos diez años, incluidas las que hiciste a tus novias, a tu mujer, a tu secretaria y tantas otras». De este modo consiguieron que entendiera el significado real de la interceptación de las telecomunicaciones. Y, en verdad, estos registros de

inteligencia ayudan a la gente a entender la labor de los servicios de inteligencia. Así que podríamos abogar por la revelación generalizada, y el caso es que si tuviera que votar este asunto ahora mismo, no tengo claro si realmente me opondría.

JULIAN

No quiero extenderme mucho sobre el tema, ya que obviamente existen casos en los que si tú estás investigando a la mafia, durante el periodo de la investigación, debes mantener tus registros en secreto. Hay circunstancias en las que esto se podría considerar legítimo. No digo que eso como política sea legítimo; estoy diciendo que es políticamente inevitable. De hecho existen demandas a favor tan convincentes políticamente —argumentos del tipo: «Estos tíos han asesinado antes, están planeando un nuevo asesinato»— que, independientemente de que pienses que la interceptación deba o no estar disponible, ésta se va a producir. No podemos ganar esa batalla política. Sin embargo este tipo de vigilancia táctica tiene la ventaja de que puede ser parcialmente regulada y el perjuicio puede limitarse a un número reducido de personas. Cuando se utiliza la interceptación táctica para la aplicación de la ley (en oposición a la inteligencia), a menudo forma parte de la recopilación de pruebas. Las pruebas terminan en los tribunales y, por ende, acaban siendo públicas. De modo que

tienes un cierto control, al menos durante algún tiempo, de lo que está pasando. Y puedes interrogar a las personas en el estrado sobre cómo se recopiló esa información y por qué deberíamos asumir que ésta es válida. Puedes vigilarla. Sin embargo la interceptación estratégica es completamente absurda. Es, por definición, interceptar a todo el mundo, de modo que ¿qué tipo de ley vas a aplicar si partes de la premisa de la interceptación masiva?

JÉRÉMIE

Este debate sobre la revelación/difusión plena me recuerda al grupo conocido con el nombre de LulzSec, que desveló 70 millones de registros de Sony —toda la información de los usuarios de Sony. Recuerdo que podías ver todas sus direcciones de correo postal y electrónico, y sus contraseñas. Creo que también había información sobre las tarjetas de crédito de 70 millones de usuarios. Como activista de los derechos fundamentales pensé: «Guau, algo va mal aquí si para defender tu punto de vista o simplemente para divertirte revelas los datos personales de la gente». Me sentí muy incómodo al ver documentadas todas esas direcciones. Pensé que este grupo sólo se estaba divirtiendo con la seguridad informática, y que lo que estaban demostrando es que una compañía tan importante y poderosa como Sony no era capaz de mantener los secretos de sus usuarios. Y que éstos, al encontrar sus nombres y

sus direcciones de correo en un buscador inmediatamente pensarían: «¡Oh! ¿Qué demonios he hecho al revelar esta información a Sony? ¿Qué significa dar información personal a una compañía?».

JACOB

Mataron al mensajero.

Ratas en la ópera

JULIAN

Tras analizar todos estos escenarios pesimistas, me gustaría que pensáramos en un posible escenario utópico. Por un lado tenemos la radicalización de la juventud de internet, y ahora internet está a punto de alcanzar la mayoría de edad. Por otro lado, tenemos varios intentos desesperados de anonimato y libertad de publicación, de libertad frente a la censura —tenemos un amplio surtido de interacciones estatales y del sector privado que están luchando contra eso—, pero imaginemos que tomamos el mejor de los caminos. ¿Cómo sería?

JACOB

Creo que consistiría en el derecho a leer y el derecho a expresarse libremente sin excepción, sin exceptuar a un solo ser humano, sin excepciones de ningún tipo, parafraseando

a Bill Hicks.[1] Él hablaba de esto en relación con la educación, el vestido y la comida, pero eso también significa, en definitiva, que toda persona tiene el derecho a leer y el derecho a expresarse libremente. Y de ahí se deriva el derecho a la expresión anónima, el derecho que te permite pagar a la gente sin interferencias de terceros, la capacidad de viajar libremente, la capacidad de corregir la información que sobre ti aparece en los sistemas. Contar con sistemas transparentes a los que podamos pedir cuentas cuando observemos algún tipo de intromisión.

ANDY

Yo añadiría la idea de que con el incremento de sistemas de tratamiento de datos y su papel en la red, y con la disponibilidad de herramientas como Tor, la criptografía y demás, la cantidad de información que puede suprimirse es bastante limitada, y los gobiernos lo saben. Saben que actuar subrepticiamente en estos tiempos significa hacerlo en el transcurso de un plazo limitado, porque tarde o temprano sus acciones acabarán siendo de dominio público, y esto es una buena cosa. Esto cambia su manera de actuar. Esto significa que saben que deberán rendir cuentas. Y también implica que se vean forzados a crear procesos internos de denuncia, como la Ley Sarbanes-Oxley (también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista), que

impone a las empresas que cotizan en la bolsa norteamericana el requisito de contar con una infraestructura de denuncia que ofrezca, a aquellos que deseen informar de un delito o de un comportamiento indebido por parte sus superiores, un procedimiento para denunciar sin sufrir represalias por parte de los acusados.[2]

JÉRÉMIE

Con respecto a lo que acaba de decir Jake, creo que debemos dejar claro que una internet libre, abierta y universal, es probablemente la herramienta más importante que tenemos para resolver los problemas globales que están en juego, que protegerla es probablemente una de las tareas claves que nuestra generación tiene entre manos, y que cuando alguien en alguna parte —ya sea un gobierno o una compañía— restringe la capacidad de la gente para acceder a la internet universal, el principal afectado es la propia internet. Es toda la humanidad la que sufre esta restricción. Y así como nosotros estamos siendo testigos de que colectivamente podemos incrementar el coste político de este tipo de decisiones, todos los ciudadanos con acceso a una internet libre pueden impedir tales comportamientos. Estamos empezando a entender que, como ciudadanos de la red, tenemos poder sobre las decisiones políticas y que podemos conseguir que nuestros representantes y nuestros gobiernos asuman mayores responsabilidades por lo que

hacen cuando adoptan malas decisiones que afectan a nuestras libertades fundamentales y a una internet libre, global y universal.

Así que creo que deberíamos ponerlo en práctica. Deberíamos intercambiar conocimientos sobre cómo hacerlo. Deberíamos continuar mejorando nuestras vías de acción, la manera en que intercambiamos tácticas sobre cómo acudir al parlamento, sobre cómo presentar lo que los políticos están haciendo, sobre cómo exponer la influencia de los lobbies de la industria en el proceso de adopción de políticas. Deberíamos seguir construyendo herramientas destinadas a capacitar a los ciudadanos en la construcción de sus propias infraestructuras encriptadas y descentralizadas, para que puedan ser dueños de sus propias infraestructuras de comunicación. Deberíamos difundir estas ideas a toda la sociedad a fin de construir un mundo mejor, y, de hecho, ya estamos en ello. Sólo debemos continuar.

JULIAN

Jake, si te fijas en personas como Evgeny Morozov y en su descripción de los problemas de internet, verás que estos asuntos ya fueron pronosticados hace años por los criptopunks.[3] No era una visión que abogara por la mera queja sobre la creciente vigilancia estatal y ese tipo de cosas, sino porque podemos y, de hecho, debemos construir las herramientas de una nueva democracia. Y podemos

construirlas con nuestras mentes, difundirlas a otra gente e involucrarnos en la defensa colectiva. La tecnología y la ciencia no son algo neutral. Hay formas concretas de tecnología que nos pueden suministrar estos derechos y libertades fundamentales tan anhelados por muchos desde hace tanto tiempo.

JACOB

Totalmente de acuerdo. Creo que lo más importante que la gente debe tener presente —especialmente los adolescentes de dieciséis a dieciocho años que deseen hacer del mundo un lugar mejor— es que ninguno de los que estamos aquí sentados, ni ninguna persona de este mundo ha nacido con los logros que se llevará a la tumba. Todos nosotros construimos alternativas. Todo el mundo aquí ha construido alternativas, y todo el mundo, especialmente con internet, está capacitado para hacerlo en el contexto en el que se mueve. Y no es que tengan obligación de hacerlo, sino que si quieren, pueden. Y si lo hacen, tendrán impacto en mucha gente, especialmente en el ámbito de internet. Construir esas alternativas tiene una amplificación, una magnificación.

JULIAN

Entonces, y me refiero a ti, si construyes algo puedes dárselo a cien mil millones de personas para que lo usen.

JACOB

O si participas en la construcción de una red anónima —como la red Tor por ejemplo— ayudas a construir la alternativa de una comunicación anónima allí donde antes no existía.

JÉRÉMIE

Se trata de compartir conocimiento libremente y facilitar canales de comunicación para que el conocimiento circule sin cortapisas, eso es lo que vosotros estáis haciendo. Tor es un software libre, que está tan ampliamente extendido en nuestros días porque hemos integrado nuestra idea de la libertad en el modo en que construimos alternativas, tecnología y modelos.

JACOB

Necesitamos un software libre para un mundo libre, y necesitamos hardware libre y abierto.

JULIAN

Pero ¿por libre quieres decir ilimitado, que la gente pueda programar sus componentes, que pueda ver cómo funciona?

JACOB

Totalmente. Necesitamos un software que sea tan libre como las leyes en una democracia, un software que todo el mundo pueda estudiar y modificar, para poder entenderlo de verdad y asegurarse de que realmente hace aquello que el usuario desea que haga. Software libre, hardware libre y abierto.[4]

JULIAN

La famosa idea de los criptopunks de «el código es la ley».

JÉRÉMIE

Es de Larry Lessig.

JULIAN

En internet lo que puedes hacer viene definido por los programas que existen, por lo que los programas activan, y por tanto el código es la ley.

JACOB

Exacto, y eso significa que puedes construir alternativas, especialmente en el ámbito de la programación, pero también en el campo de la impresión 3D o incluso en el ámbito social como los «espacios hacker», que ya existen.[5] Puedes ayudar a construir alternativas y lo esencial es que puedas llevártelas a casa e integrarlas en un proceso de

normalización, un proceso en el que la sociedad se habitúe a construir sus propios objetos tridimensionales, a modificar su propio software y donde todos tomen conciencia de que si alguien les impide hacerlo, entonces, quien quiera que sea el que se lo impida, no está ofreciendo acceso a internet, está ofreciendo acceso a una red de filtros o a una red de censura, y, eso en realidad significa que están incumpliendo su deber de protección.

Eso es lo que todos nosotros hemos hecho con nuestras vidas y la gente debería saber que tienen la capacidad de hacerlo para las futuras generaciones y para esta generación. Por eso estoy aquí —porque si no apoyo a Julian en este momento, en lo que está pasando ¿qué tipo de mundo estoy construyendo? ¿Qué tipo de mensaje envío cuando dejo que una panda de cerdos me presione? Ni hablar, de ninguna manera. Tenemos que construir y tenemos que cambiar eso. Como dijo Gandhi: «Tú tienes que ser el cambio que quieres ver en el mundo». Pero también tienes que ser el problema que quieres ver en el mundo.[6] Es una cita de *Softer World*, no es la misma que la de Gandhi, pero creo que es importante llevarla a cabo, y también que la gente necesita saber que no basta con sentarse a esperar ociosamente, deben lanzarse a la acción y, con suerte, lo harán.[7]

ANDY

Creo que estamos viendo una buena oportunidad de que la gente pueda llegar aún más lejos que nosotros, y las alternativas provienen de personas que están insatisfechas con la situación que encuentran o con las opciones que tienen.

JULIAN

¿Nos puedes hablar un poco del papel del Club del Caos Informático [CCC, en sus siglas en inglés] en este contexto?

ANDY

Y dale con el CCC... *fnord*.[8]

JULIAN

Lo cierto es que es único en el mundo.

ANDY

El CCC es una organización galáctica de piratas informáticos que promueve la libertad de información, la transparencia de la tecnología, y que se preocupa de la relación entre el hombre y el desarrollo tecnológico, es decir, de que la sociedad y el desarrollo interactúen entre sí.

JULIAN

Ha adquirido un sesgo político.

ANDY

El CCC se ha convertido en una especie de foro dentro del escenario hacker con unos cuantos miles de miembros y con cierta base en Alemania. Nosotros no nos sentimos habitantes de Alemania sino de internet, lo cual ayuda en gran parte a entender nuestra filosofía, y también atrae. Estamos muy bien relacionados a través de la red con otros grupos de hackers creados en Francia, en América y otros lugares.

JULIAN

¿Y por qué crees que éste empezó en Alemania? El corazón está en Alemania, pese a haberse expandido al resto del mundo.

ANDY

Los alemanes siempre tratan de estructurarlo todo.

JÉRÉMIE

La ingeniería alemana es mejor.

JULIAN

Pero creo que no es sólo eso. Es que esto es Berlín y representa la caída del Este.

ANDY

Tiene que ver con múltiples factores. Alemania ha cometido el peor acto que un país puede cometer contra el ser humano, de modo que tal vez sea un poco más inmune a emprender este tipo de acciones de nuevo, acciones como iniciar una guerra con otros países. Nosotros lo hemos hecho todo, hemos pasado por ello, hemos sido duramente castigados y teníamos que aprender de la experiencia, y, de hecho, este pensamiento descentralizado y este comportamiento antifascista —como tratar de evitar un Estado totalitario—, se sigue enseñando en los colegios alemanes, porque lo hemos experimentado hasta el peor de los niveles. Así que pienso que eso constituye una parte importante para entender al CCC, diría que en parte es una suerte de fenómeno alemán. Wau Holland, el creador y fundador del club, también estaba profundamente convencido de esto. Yo vi a su padre frente a su tumba (su hijo murió antes que él), y sus palabras no fueron precisamente agradables. Dijo: «...y que no vuelvan a producirse nunca acciones totalitarias y bélicas en suelo alemán». Tal fue el comentario del padre de Wau cuando enterró a su hijo, y en mi opinión, eso explica en gran medida la determinación de Wau de influir y ayudar a los demás, de actuar en paz con el prójimo, de difundir ideas y no limitarlas, y de actuar sin hostilidad y con espíritu de cooperación.

Y también la idea de crear cosas conjuntamente, como el

movimiento del software libre y demás. Ha calado hondo y se ha integrado en el ideario de los criptopunks americanos y en el del WikiLeaks de Julian Assange, etcétera. Se ha convertido sin duda en algo global que integra actitudes culturales muy diversas y tremendamente descentralizadas de hackers suizos, alemanes, italianos... Y eso es bueno. Los hackers italianos se comportan de una manera completamente distinta a la de los hackers alemanes, estén donde estén, tienen que hacer una buena comida; los hackers alemanes necesitan tener todo muy bien estructurado. No digo que unos sean mejores que los otros, sólo estoy diciendo que cada una de estas culturas descentralizadas tiene su parte única y preciosa. En la conferencia de hackers italiana puedes ir a la cocina y encontrarás un lugar maravilloso; en el campamento hacker alemán verás un maravilloso internet, pero es mejor no acercarse a la cocina. Con todo, lo esencial es que estamos creando. Y creo que todos nos encontramos inmersos en una especie de conciencia común totalmente alejada de nuestra identidad nacional —de sentirnos alemanes o italianos o americanos o de cualquier otro lugar—, sólo vemos que queremos resolver problemas, queremos trabajar juntos. Vemos la censura de internet, esta lucha de los gobiernos en contra de las nuevas tecnologías, como una especie de situación evolutiva que tenemos que superar.

Estamos en el camino de identificar soluciones y no

sólo problemas, y esto es bueno. Probablemente tendremos que seguir plantando cara a un montón de mierda en los años venideros, pero por fin hay una generación emergente de políticos que no ve a internet como un enemigo, y que entiende que internet es parte de la solución, y no parte del problema. Todavía tenemos un mundo edificado sobre las armas, sobre los secretos del poder, sobre una base puramente económica... Pero eso está cambiando y creo que nosotros desempeñamos un papel muy importante en el diseño de las políticas actuales. Podemos debatir los asuntos de manera polémica, y esto es algo que el CCC lleva haciendo desde hace tiempo. No somos un grupo homogéneo, tenemos opiniones diferentes. Yo valoro que podamos sentarnos juntos a dialogar y que las respuestas no salgan a la primera de cambio, nos limitamos a plantear preguntas, ponemos nuestras múltiples ideas sobre la mesa y sacamos conclusiones. Ése es el proceso que debemos plantear y para el que necesitamos internet.

JULIAN

Antes planteé la pregunta de cómo sería el mejor de los futuros posibles. Autoconocimiento, diversidad y redes de autodeterminación. Una población global altamente cualificada —y con esto no me refiero a estudios oficiales, sino a personas bien formadas en la comprensión del funcionamiento de la civilización humana a nivel político,

industrial, científico y psicosocial—, gracias al libre intercambio de información, que estimule la creación de culturas dinámicas y la máxima diversificación del pensamiento individual, una mayor autodeterminación tanto regional como de grupos de interés capaces de interconectarse con rapidez e intercambiar valor por encima de las fronteras geográficas. Y tal vez todo ello se haya manifestado en la primavera árabe y en el activismo panárabe potenciado a través de internet. En nuestro trabajo con Nawaat.org, organismo que creó Tunileaks, —que burlando la censura filtró los cables del Departamento de Estado que impulsaron el Túnez prerrevolucionario— vimos de primera mano el extraordinario poder de la red para mover la información allí donde se necesita, y fue tremendamente gratificante haber estado en una posición que, gracias a nuestros esfuerzos, nos permitiera participar en lo que allí empezaba a gestarse.[9] Yo no percibo esa lucha por la autodeterminación como una lucha distinta a la nuestra.

Esta trayectoria positiva comportaría el autoconocimiento de la civilización humana, pues el pasado no puede destruirse. Comportaría la erradicación de los Estados neototalitarios, gracias a la libre circulación de la información y a la capacidad de las personas de comunicarse unas con otras privadamente y de conspirar en contra de ese tipo de tendencias, así como la capacidad de transferir sin cortapisas capitales pequeños desde aquellos lugares

considerados inhóspitos para los seres humanos.

Partiendo de esos cimientos podemos construir una gran variedad de sistemas políticos. La utopía sería para mí una distopía si hubiera sólo uno de estos factores. Creo que los ideales utópicos deben integrar una diversidad de sistemas y modelos de interacción. Si os fijáis en el caótico desarrollo de nuevos productos culturales e incluso en los derroteros que ha tomado el lenguaje, y en las subculturas que conforman sus propios mecanismos de interacción potenciados por internet, entonces sí, puedo ver que, en efecto, eso sí abre un posible camino de esperanza.

Pero también creo en todas las tendencias de la probabilidad encaminadas hacia la homogeneización, a la universalidad, a que la civilización humana al completo derive en un solo mercado, lo cual significa que tendrás factores de mercado ordinarios como un líder de mercado, un segundo, un tercer jugador de nicho y luego rezagados que resultan irrelevantes, para cada servicio y producto. Creo que tal vez implique homogeneización masiva del lenguaje, masiva homogenización cultural, estandarización masiva dirigida a que estos rápidos intercambios sean más eficaces. De modo que pienso que un escenario pesimista también puede ser bastante probable, y que el Estado de vigilancia transnacional y las interminables guerras teledirigidas se ciernen sobre nosotros.

De hecho, me viene a la memoria el día en que me colé

en el teatro de la Ópera de Sydney para ver Fausto. La Ópera de Sydney es un lugar precioso por la noche, sus grandiosos interiores y las luces refulgiendo sobre el agua y en el cielo de la noche. Al cabo de un rato salí a tomar el aire y escuché la charla de tres mujeres que estaban apoyadas en la barandilla contemplando la bahía. La mujer de más edad hablaba de los problemas que tenía en su trabajo, resultó que trabajaba para la CIA como agente de los servicios de inteligencia, y, por lo visto, había presentado una queja al comité de selección del senado en materia de inteligencia y otras historias... Y ella contaba todo esto en un tono apenas audible a su sobrina y a la otra mujer. Yo pensé: «Entonces es cierto. Los agentes de la CIA realmente salen a divertirse a la Ópera de Sydney». Y luego volví la vista hacia el interior del edificio, a través de los robustos paneles de cristal del frente, y allí, en medio de aquel solitario refinamiento palaciego, vi una rata de agua que había logrado colarse en el interior del teatro de la ópera y que correteaba sin tregua ni dirección encaramándose a las mesas cubiertas con delicados manteles de lino y comiéndose el menú del teatro de la ópera, y luego la vi saltando al mostrador de los tickets y pasárselo realmente en grande. Y lo cierto es que creo que tal vez sea ése el escenario más probable para el futuro: una estructura totalitaria extremadamente cerrada, homogeneizada, posmoderna y transnacional dotada de una complejidad increíble, ridícula y degradada, y dentro de esa

increíble complejidad un espacio donde sólo las ratas más listas pueden entrar.

Es un punto de vista esperanzador en la trayectoria negativa, siendo la trayectoria negativa un Estado de vigilancia transnacional, infestado de *drones*, el neofeudalismo interconectado de la élite transnacional —no en el sentido clásico, sino en el de una compleja interacción pluripartidista surgida a raíz del levantamiento conjunto de las distintas élites nacionales frente a sus respectivos pueblos, y de la ulterior fusión de todas ellas. Todas las comunicaciones serán vigiladas, permanentemente grabadas, permanentemente rastreadas, cada individuo en todas y cada una de sus interacciones será permanentemente identificado como tal individuo por este nuevo *Establishment*, desde su nacimiento hasta su muerte. Se trata de un cambio fundamental que viene gestándose en el transcurso de estos diez últimos años y que puede haberse consolidado ya. Creo que eso sólo puede generar una atmósfera tremendamente controladora. Si toda la información recopilada sobre el mundo fuera pública, tal vez eso podría reequilibrar la dinámica del poder y permitirnos, como civilización global, moldear nuestro destino. Pero sin un cambio drástico esto no sucederá. La vigilancia masiva se aplica desproporcionadamente sobre la mayoría de nosotros, transfiriendo poder a aquellos inmersos en un plan que, pese a todo, creo, tampoco les permitirá disfrutar gran cosa de

este nuevo mundo feliz. Este sistema además coexistirá con una nueva raza de armas teledirigidas que eliminarán las fronteras claramente definidas que hoy conocemos, pues tales fronteras son producto de la impugnación de límites físicos, impugnación que se convierte en un estado de guerra perpetua cuando las redes de influencia de los vencedores empiezan a zarandear al mundo en busca de concesiones. Y, paralelamente, esta gente acabará enterrada bajo la matemática imposible de la burocracia.

¿Cómo puede una persona normal ser libre en un sistema como ése? Simplemente no puede. Es imposible. No digo que exista un sistema en el que se pueda ser completamente libre, pero las libertades que biológicamente hemos adquirido, y las libertades que hemos conquistado socialmente, serán eliminadas prácticamente en su totalidad. De modo que creo que las únicas personas capaces de conservar la libertad que teníamos, digamos, hace veinte años —pues el Estado de vigilancia ya ha eliminado unas cuantas, aunque todavía no nos hayamos enterado—, son aquellas que posean una gran formación en los entresijos de este sistema. Sólo una élite rebelde y altamente tecnificada podrá ser libre, estas ratas listas que corretean por el teatro de la ópera.

Notas

Prólogo

[1]. DPI, Inspección profunda de paquetes, una sofisticada tecnología que permite espiar y rastrear las comunicaciones del internauta.

¿Qué es un *criptopunk*?

[1]. Dicho de otro modo, criptografía, término griego que significa escritura secreta, o uso de la comunicación en clave.

[2]. «El Oxford English Dictionary actualiza algunas entradas e incorpora nuevas palabras; Bada-Bing (voilà!), Cypherpunk (criptopunk) y Wi-Fi (conexión inalámbrica) en el OED», *ResourceShelf*, 16 de septiembre de 2006: http://web.resourceshelf.com/go/resourceblog/43743 (último acceso 24 de octubre de 2012).

Participantes en el debate

[1]. WikiLeaks: http://wikileaks.org.

[2]. Para ampliar información sobre el archivo Rubberhorse véase: *The Idiot Savants Guide to the Rubberhorse*, Suelette Dreyfus: http://marutukku.org/current/src/doc/maruguide/t1.html (última entrada 14 de octubre de 2012).

[3]. Para ampliar información sobre el libro *Underground*, véase: http://underground-book.net.

Para ampliar información sobre la película *Underground: La Historia de Julian Assange,* véase la base de datos de películas de internet: http://www.imdb.com/title/tt2357453/ (entrada 20 de octubre de 2012).

[4]. Noisebridge es un *hacker-espacio* con base en San Francisco, un proveedor de infraestructura a proyectos de carácter técnico-creativo cogestionado por sus miembros: https://www.noisebridge.net/wiki/Noisebridge.

Chaos Computer Club Berlín es la organización de Berlín del Club del Caos Informático, véase: https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin

[5]. Proyecto Tor: https://www.torproject.org.

[6]. El Club del Caos Informático es la mayor asociación europea de hackers. Sus actividades abarcan desde la investigación y exploración técnica a campañas, eventos, publicaciones y asesoramiento: http://www.ccc.de.

[7]. EDRI: http://www.edri.org.

[8]. ICANN: http://www.icann.org.

[9]. buggedplanet: http://buggedplanet.info.

[10]. Cryptophone: http://www.criptophone.de.

[11]. La Quadrature du Net: http://laquadrature.net.

[12]. *Collateral Murder*: http://www.collateralmurder.com.
The Iraq War Logs: http://wikileaks.org/irq.
The Afghan War Diary: http://wikileaks.org/afg.
Cablegate: http://wikileaks.org/cablegate.html.

[13]. «El comité del Congreso convoca una audiencia sobre prevención y castigo de filtraciones de seguridad nacional». Comité de reporteros para la libertad de prensa, 11 de julio de 2012: http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent (último acceso 21 de octubre de 2012).

[14]. Para ampliar información sobre el gran jurado de WikiLeaks ver cronología de la periodista Alexa O'Brien. http://www.alexaobrien.com/timeline_us_versus_manning_as (último acceso 22 de octubre de 2012).

[15]. «El trato a Bradley Manning fue cruel e inhumano, dictamina el principal responsable de la ONU en materia de tortura». *The Guardian*, 12 de marzo de 2012. http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un (último acceso 24 de octubre de 2012).

[16]. WikiLeaks: los culpables «deberían ser condenados a pena de muerte». *Telegraph*, 1 de diciembre de 2010: http://www.telegraph.co.uk/news/worldnews/wikileaks/81729 guilty-parties-should-face-death-penalty.html (último acceso 22 de octubre de 2012).

[17]. «La CIA crea un cuerpo especial para evaluar el impacto de los cables norteamericanos filtrados por WikiLeaks». *Washington Post*, 22 de diciembre de 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/ AR2010122104599. html?hpid= topnews&sid= ST2010122105304 (último acceso 22 de octubre de 2012).

[18]. «WikiLeaks lucha por seguir en la red tras la retirada de su dominio por parte de una compañía americana». The *Guardian*, 3 de diciembre de 2010: http://www.guardian.co.uk/media/blog/2010/dec/o3/wikileaks knocked-off-net-dns-eveydns (último acceso 23 de de octubre de 2012).

[19]. «No Mires, no Leas: El gobierno advierte a sus trabajadores que se mantengan lejos de los documentos de WikiLeaks». *The New York Times*, 4 de diciembre de 2012: http://www.nytimes.com/2010/12/05/world/5restrict.html?hp&_r=2& (último acceso 23 de octubre de 2012).

[20]. «Bloqueo bancario», WikiLeaks: http://www.wikileaks.org//Banking-Blockade.html (último acceso 22 de octubre de 2012).

[21]. Se recomienda la lectura del diario de detenciones de Jacob en Democracy Now! «William Binney, informante de la Agencia de Seguridad Nacional, en relación con la creciente vigilancia del estado», Democracy Now!, 20 de abril de 2012: http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william (ultimo acceso a ambos enlaces: 23 de octubre de 2012).

[22]. El caso se conoce oficialmente como Asunto de la Orden 2703(d) concerniente a las cuentas de Twitter: @Wikileaks @Rop_G, @IOERROR y @birgittaj.

[23]. «Citaciones secretas identifican correos electrónicos». *Wall Street Journal*, 9 de octubre de 2011: http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (último acceso 22 de octubre de 2012).

[24]. «Twitter obligado a ceder información en el caso WikiLeaks». *The New York Times*, 10 de noviembre de 2011: https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1 (último acceso 22 de octubre de 2012).

[25]. «ACLU & EFF se unen para impugnar el fallo que ratifica la ocultación de información en el caso Twitter/WikiLeaks». Comunicado de prensa de la Fundación Fronteras Electrónicas, 20 de enero de 2012: https://eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitterwikileaks-case (último acceso 22 de octubre de 2012).

Mayor comunicación versus mayor vigilancia

[1]Ésta fue la protesta del 6 de abril del 2008 en apoyo a la huelga suspendida de los trabajadores del grupo textil Mahalla al-Kobra. Poco antes de la huelga, el Movimiento de la juventud del 6 de abril se constituyó como grupo de Facebook, con el fin de animar a los egipcios a realizar actos de protesta en El Cairo y en otras ciudades coincidiendo con la acción industrial en Mahalla. Las protestas no tuvieron el éxito esperado y los promotores del grupo de Facebook, Esraa Abdel Fattah, Ahmed Rashid y Ahmed Maher entre otros, fueron arrestados. Maher fue objeto de torturas para sonsacarle su contraseña de Facebook. El movimiento de la juventud del 6 de abril continuó su andadura desempeñando un importante papel en la revolución egipcia de 2011. Véase «Activistas de El Cairo usan Facebook para agitar al régimen», *Wired*, 20 de octubre de 2008: http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?currentPage=all (último acceso 23 de octubre de 2012).

[2]. «Cómo protestar con inteligencia», autores anónimos, distribuido a principios del décimo octavo día del levantamiento que acabó con el Presidente Mubarak (árabe): http://itstime.it/Approfondimenti/EgyptianRevolutionManua Extractos del documento fueron traducidos al inglés y publicados bajo el título *Plan de acción de los Activistas Egipcios*, traducido por *Atlantic* el 27 de enero de 2011: http://www.theatlantic.com/international/archive/2011/01/egy activists-action-plan-translated/70388 (último acceso a ambos enlaces 23 de octubre de 2012).

[3]. El Panóptico fue un centro penitenciario concebido por el filósofo Jeremy Betham en 1787, con el fin de que un solo vigilante pudiera vigilar al tiempo a todos los prisioneros, al estar todos en su mismo campo visual. Jeremy Bentham (editado por Miran Bozovic) *The Panopticon Writings*, (Verso, 1995), disponible online en: http://cartome.org/panopticon2.htm (último acceso 22 de octubre de 2012).

[4]. Johannes Gutenberg (1398-1468) fue un orfebre alemán que inventó la imprenta mecánica de tipos móviles, invento que generó algunas de las revueltas sociales más importantes de la historia. La invención de la imprenta es la analogía histórica más parecida a la invención de Internet.

[5]. John Gilmore es uno de los primeros criptopunks y fundador de la *Electronic Frontier Foundation* (Fundación de Fronteras Electrónicas) y activista y defensor de las libertades civiles. La frase citada por Andy fue publicada por primera vez en el artículo «La Primera Nación en el Ciberespacio» de la revista *Time* el 6 de diciembre de 1993. Véase la página web de John Gilmore: http://www.toad.com/gnu (último acceso 22 de octubre de 2012).

[6]. «Las tecnologías patentadas son tipos de sistemas, herramientas o procesos técnicos desarrollados por y para una entidad o negocio concretos... Las ideas desarrolladas y remitidas por los empleados suelen considerarse propiedad intelectual del empleador, lo cual le permite adueñarse de la tecnología patentada». Definición extraída de wiseGEEK: http://www.wisegeek.com/what-is-proprietary-technology.htm (último acceso 22 de octubre de 2012).

[7]. Cory Doctorow: «La inminente guerra a la computación de uso general». Boingboing, 10 de junio de 2012 (basada en el discurso de apertura efectuado en el Congreso del Club del Caos Informático, en diciembre de 2011): http://boingboing.net/2012/01/10/lockdown.html (último acceso 15 de octubre de 2012).

[8]. Stuxnet es un gusano informático tremendamente sofisticado que, según la opinión general, fue conjuntamente desarrollado por EE.UU. e Israel con el fin de atacar los equipos Siemens presuntamente utilizados por Irán en procesos de enriquecimiento de uranio. Véase la información que aparece en Wikipedia sobre el Stuxnet: http://en.wikipedia.org/wiki/Stuxnet.

Véase también: «WikiLeaks: EE.UU. aconsejó el sabotaje de emplazamientos nucleares iraníes por parte de un grupo de expertos alemán». *The Guardian*, 18 de enero de 2011: http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear.

WikiLeaks desarrolló uno de los primeros informes sobre los efectos que ahora se consideran consecuencia del Stuxnet: el accidente nuclear en las instalaciones nucleares de Natanz, Irán. Véase «Grave accidente nuclear puede estar detrás de la misteriosa dimisión del jefe iraní de energía nuclear», WikiLeaks 17 de julio de 2009: http://wikileaks.org/wiki/Serious_muclear_accident_may-lay_behind_Iranian_nuke_chief%27s_mystery_resignation. Existen pruebas de empresa privada de inteligencia global Stratfor, filtradas por WikiLeaks que sugieren la posible participación de Israel. Véase email ID 185945, los archivos de inteligencia global: http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (último acceso

a todos los enlaces 16 de octubre de 2012).

La militarización del ciberespacio

[1]. Pentesting, traducido generalmente como test de intrusión, es un tipo de auditoría de seguridad para efectuar ataques de manera autorizada a un sistema o red informática, del mismo modo en que lo haría un usuario desautorizado, con el fin de evaluar la seguridad del sistema. Los investigadores de seguridad se reclutan a menudo entre la comunidad hacker para realizar tests de intrusión en sistemas de seguridad.

[2]. *Capturar la bandera* es originalmente un juego al aire libre en el que suelen participar dos equipos que defienden, cada uno desde su base, sus respectivas banderas. El objetivo consiste en conseguir la bandera del equipo contrario y regresar a la base. En las conferencias de hackers se juega una versión de este juego en la que los equipos atacan y defienden ordenadores y redes.

[3]. La copa Sysadmin es una contracción de copa de Administradores de Sistemas en inglés. Un administrador de sistemas es una persona del sector IT encargada de mantener y operar un sistema informático o una red. Jacob dice que el ejercicio era como un torneo para administradores de sistemas.

[4]. «Aaron alega que la criptografía protege la privacidad, el comercio»; USIS Washington File, 13 de octubre de 1998: http://www.fas.org/irp/news/1998/10/98101306_clt.html (último acceso 21 de octubre de 2012).

[5]. Página web Acuerdo Wassenaar: http://www.vassenaar.org (último acceso 21 de octubre de 2012).

[6]. Andy se refiere a una serie de desarrollos que tuvieron lugar en las primeras criptoguerras de la década de los noventa. Cuando los activistas del movimiento criptopunk empezaron a difundir importantes herramientas criptográficas como software libre, la Administración estadounidense dio pasos para impedir su utilización. Clasificó a la criptografía de «munición» y restringió su exportación; trató de introducir tecnologías rivales que fueron deliberadamente quebrantadas para que las fuerzas de seguridad pudieran desencriptar la información; y también trató de introducir el controvertido plan «de custodia de claves». Durante un corto periodo, a principios del siglo XXI, era comúnmente aceptado que estos esfuerzos habían sido rechazados de plano. Sin embargo en la actualidad se está librando una segunda cripto-guerra con esfuerzos técnicos y legislativos para relegar o marginar el uso de la criptografía.

[7]. El cálculo de la muestra hacía referencia a los ciento noventa y seis mil con cuatro millones de minutos de llamadas de red fija que se hicieron en Alemania en el año 2010, digitalizadas con un códec de voz de 8 kbps, representaban un total de 11,784 Petabites (Pb), y redondeado tras añadir otros datos generales totalizaba unos 15 Pb. Calculando un coste aproximado de almacenaje de 500.000 dólares (500kUSD) por Pb, representa un total de 7,5 millones de dólares o unos 6 millones de euros. A todo esto hay que añadir los costes para el establecimiento del centro de datos, la potencia de procesamiento, las conexiones y la mano de obra. Incluso en el caso de que se añadieran las ciento un mil millones de llamadas de móviles efectuadas en Alemania el año 2010, con otros 50pbt y 18.3 millones de euros más, el precio seguiría siendo inferior al de un solo avión militar como el Eurofighter (90 millones de euros) o el F22 (150 millones de dólares americanos).

[8]. Para ampliar información sobre VASTech, véase buggedplanet: http://buggedplanet.info/index.php?title=VASTECH (último acceso octubre de 2012).

[9]. El escándalo de escuchas ilegales internas por parte de la ASN se ha convertido en el caso de vigilancia masiva más grave de la historia de EE.UU. La ley de Vigilancia de Inteligencia Exterior de 1978 (también conocida como la FISA por sus siglas en inglés) ilegalizó el espionaje por parte de agencias gubernamentales a ciudadanos estadounidenses sin una orden judicial. Tras el 11 de septiembre, la Agencia de Seguridad Nacional empezó a violar la FISA de manera reiterada, amparándose en una orden ejecutiva de carácter secreto dictada por George W. Bush. La administración Bush se declaró competente para hacer esto a tenor de una ley de emergencia aprobada por el Congreso: La Autorización para el Uso de la Fuerza Militar y la Ley Patriota, que fue secreta hasta que en el año 2005 el diario *The NewYork Times* se hizo eco de su existencia. Véase «Bush autoriza el espionaje de llamadas internas sin orden judicial». *The New York Times* 16 de diciembre de 2005: http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Reporteros de *The New York Times* fueron contactados por un informante anónimo de la ASN. Poco después se supo que se trataba del ex-abogado del Departamento de Justicia, Thomas Tamm. En el año 2004 el editor ejecutivo de *The New York Times*, Bill Keller, accedió a la petición de la administración Bush de no publicar la historia en el plazo de un año, hasta que Bush fuera reelegido. En el año 2005 el

diario se apresuró a hacerla pública tras enterarse de la existencia de múltiples documentos desclasificados del Pentágono en los que se justificaba este tipo de actuaciones sin necesidad de orden de judicial. La administración Bush negó que existiera algún tipo de ilegalidad en el programa de la Agencia de Seguridad Nacional. El Departamento de Justicia inició de inmediato una investigación sobre la fuente de la denuncia, en la que participaron veinticinco agentes federales y cinco fiscales. Importantes miembros del partido republicano solicitaron el procesamiento judicial de *The New York Times* amparándose en la Ley de Espionaje.

Tras la publicación del diario, nuevos informantes recurrieron a la prensa presentando de manera gradual un cuadro detallado de la anarquía y el abuso que existía en los altos cargos de la ASN. Se presentaron múltiples demandas colectivas encabezadas por grupos de apoyo como La Unión de Libertades Civiles y (ACLU) y la Fundación de Fronteras Electrónicas (o EFF). En uno de estos litigios: ACLU vs NSA, la demanda no se admitió a trámite alegando que los demandantes no podían probar que habían sido espiados personalmente. En otro caso Hepting v AT&T, un denunciante de AT&T presentó una declaración jurada en la que relataba el grado de cooperación de AT&T con el programa de espionaje doméstico. Véase el apartado Hepting v. AT&T en el sitio web de EFF: https://www.eff.org/cases/hepting.

Mark Klein era uno de los demandantes del caso Hepting v. AT&T. Ex empleado de AT&T, que trabajaba en Folsom, San Francisco, su declaración jurada a la Fundación de Fronteras Electrónicas en el caso Hepting v. AT&T, reveló la existencia del «cuarto 641A» una instalación de interceptación estratégica operada por AT&T para la Agencia de Seguridad Nacional. La instalación ofrecía acceso a enlaces de fibra óptica que contenían el tráfico troncal de Internet, dada su capacidad para involucrarse en la vigilancia de todo el tráfico de red que pasara por el edificio, tanto foráneo como interno. Otro denunciante de la ASN, William Binney, ha estimado que existen unas 20 instalaciones como esa, todas situadas en puntos clave de la red de telecomunicaciones de Estados Unidos.

La declaración jurada de Klein nos aporta información importante sobre el tipo de programa de vigilancia de la ASN, información que ha sido ratificada por varios informantes de la ASN. Esto es un ejemplo de «interceptación estratégica», todo el tráfico que pase por Estados Unidos es copiado y almacenado indefinidamente. Además se sabe con certeza que el tráfico de datos interno también se intercepta y se almacena, pues, desde el punto de vista de la ingeniería, cuando manejas tal volumen de información es imposible dejar fuera el tráfico para el que se requeriría la orden judicial establecida por la FISA. La actual interpretación legal de la FISA sostiene que una

«interceptación» sólo tiene lugar cuando se «accede» a la base de datos de la ASN en busca de una comunicación interna previamente interceptada y almacenada por la ASN, sólo en esta fase se requiere una orden judicial. Los ciudadanos estadounidenses deben asumir que todo el tráfico de sus telecomunicaciones (incluidas llamadas de voz, mensajes cortos, correos electrónicos y navegación web) es controlado y almacenado para siempre en los centros de datos de la Agencia de Seguridad Nacional.

En el año 2008, en respuesta a la cantidad de litigios suscitados a raíz del escándalo de las escuchas telefónicas, el Congreso de EE.UU. presentó enmiendas a la ley FISA de 1978 que el presidente firmaría con carácter urgente. Esto sentó las bases para garantizar una «inmunidad retroactiva» tremendamente controvertida frente a las demandas de violación de los derechos contenidos en esta ley. El senador Barack Obama, durante su campaña presidencial hizo de la «transparencia» uno de los baluartes de su programa, comprometiéndose a proteger a los informantes. Sin embargo, cuando accedió a la presidencia en 2009, su Departamento de Justicia continuó con las mismas políticas iniciadas por la administración Bush, frustrando las expectativas de los demandantes del caso Hepting y otros al aplicar la garantía de «inmunidad retroactiva» a AT&T. Si bien su Departamento de Justicia no llegó a averiguar la fuente original de la historia publicada por *The New York*

Times, sí consiguió destapar a varios denunciantes surgidos a posteriori. Uno de ellos era Thomas Drake, un antiguo ejecutivo de la Agencia de Seguridad Nacional, que llevaba años presentando quejas internas a los Comités Generales de Inteligencia del Congreso sobre la corrupción y el despilfarro del «pionero» programa de la ASN. Las quejas internas se eliminaban al igual que los funcionarios que las planteaban. Tras el artículo de *The New York Times*, Drake reveló la flamante historia al diario *Baltimore Sun*. Fue procesado por el gran jurado, que le declaró «enemigo del Estado», y le acusó de violar la Ley de Espionaje. Véase «*The Secret Sharer*» (el compartidor secreto). *The New Yorker*, 23 de Mayo de 2011: http://www.newyorker.com/reporting/2011/05/23/110523fa_fac currentPage=all.

El proceso contra Drake fracasó tras las presiones públicas en junio de 2011, y después de varios intentos fallidos de negociar con Drake la condena que se le imputaba, el Departamento de Justicia se vio obligado a condenarlo por un delito menor con pena de un año de libertad vigilada.

Las secuelas del escándalo de las escuchas continúan. La Unión de Libertades Civiles sigue litigando en contra de la constitucionalidad de las enmiendas de la FISA del año 2008 en el caso Amnesty et. al. v. Clapper. Véase «Impugnación de la Enmienda a la FISA», ACLU 24 de septiembre de 2012:

http://www.aclu.org/national-security/amnesty-et-al-v-clapper.

En el caso Jewel versus la ASN, la EFF trata de poner fin a la vigilancia indiscriminada por parte de la ASN. El caso fue desestimado en el año 2009, cuando la administración Obama decretó su inmunidad en cuestiones de seguridad nacional. Véase la página de la EFF sobre Jewel versus la ASN. https://www.eff.org/cases/jewel. Sin embargo, La Corte de Apelación del Noveno Circuito permitió reabrir el caso en diciembre del año 2011. Thomas Drake y los informadores de la ASN, William Binney y J. Kirk Wiebe están aportando pruebas fehacientes al caso de Jewel contra la ASN. La administración Obama —que había puesto en marcha una plataforma de transparencia gubernamental— procesó a más informantes bajó los auspicios de la Ley de Espionaje que todas las administraciones anteriores juntas (último acceso a todos los enlaces de esta nota 23 de octubre de 2012).

[10]. Véase entrada para el sistema Eagle en buggedplantet: http://buggedplanet.info/index.php?title=AMESYS#Srategic_.28.22Massi ve.22.29_Appliances (último acceso 22 de octubre de 2012).

Combatir la vigilancia total con las leyes del hombre

[1]. «Tribunal alemán ordena la eliminación de las telecomunicaciones almacenadas», BBC, 2 de marzo de 2010: http://news.bbc.co.uk/1/hi/world/europe/8545772.stm (último acceso 15 de octubre de 2012).

[2]. La directiva 2006/24/CE del Parlamento Europeo y Consejo exige a los países de la Unión el almacenamiento de las telecomunicaciones de los ciudadanos europeos de seis a veinticuatro meses. Fue al trasladar esta directiva a la legislación alemana cuando ésta fue declarada inconstitucional en Alemania. En Mayo de 2012 la Comisión de la Unión Europea remitió a Alemania al Tribunal Europeo de Justicia por no cumplir con la Directiva (véase el comunicado de prensa de la Comisión: http://europa.eu/rapid/press-release_IP-12-530_en.htm (último acceso 15 de octubre de 2012).

[3]. Véase «Suecia aprueba ley de escuchas», BBC, 19 de junio de 2008:

http://news.bbc.co.uk/1/hi/world/europe/7463333.stm.

Para ampliar información sobre FRA-lagen, véase Wikipedia: http://en.wikipedia.org/wiki/FRA_law (ambos enlaces visitados el 10 de octubre de 2012).

[4]. Metadata significa «datos sobre datos». En el contexto que nos ocupa, los metadatos hacen referencia a información distinta de la del contenido de la comunicación electrónica. Es la parte frontal del sobre, y no lo que éste contiene. La vigilancia de metadatos no busca los contenidos de los correos electrónicos sino la información que rodea a dichos contenidos: a quién se envía el correo o de quién parte, las direcciones IP (y por tanto la ubicación del remitente y del destinatario), las horas y las fechas de cada correo, etc. No obstante la cuestión es que la tecnología necesaria para interceptar metadatos es la misma tecnología que aquella que se utiliza para interceptar los contenidos. Si concedes a alguien el derecho a vigilar tus metadatos, el equipo también interceptará el contenido de tus comunicaciones. Además, la mayoría de la gente no se da cuenta de que los «metadatos constituyen un contenido añadido», cuando se reúnen todos los metadatos de un individuo, éstos te ofrecen una foto increíblemente detallada de las comunicaciones de dicho individuo.

[5]. Amesys forma parte del grupo Bull, antaño competencia de la filial alemana de IBM Dehomag en la venta de sistemas de tarjetas perforadas a los nazis. Véase el ensayo *IBM and the Holocaust* (Crown Books, 2001) de Edwin Black.

Para ampliar información sobre el espionaje de Gaddafi a los libios en Reino Unido con equipos de vigilancia de Amesys, véase: «Exclusiva, cómo Gaddafi espiaba a los Padres de la nueva Libia» OWNI.eu, 1 de diciembre de 2011: http://owni.eu/2011/12/01/exclusive-how-gaddafi-spided-on-the-fathers-of-the-new-lybia (último acceso 22 de octubre de 2012).

[6]. WikiLeaks empezó a revelar los Archivos Espía, mostrando la magnitud de la vigilancia masiva en diciembre de 2011. Pueden leerse en http://wikileaks.orgs/the-spyfiles.html

[7]. Más información en buggedplanet: http://buggedplanet.info/index.php?title=LY

[8]. El Congreso de Comunicación del Caos es un encuentro anual del escenario hacker internacional organizado por el Club del Caos Informático.

[9]. Jacob se refiere a ZTE, uno de los dos productores chinos (el otro es Huawei) de componentes electrónicos, y sobre los que existe la sospecha generalizada de que contienen «puertas traseras» (*backdoors*). Jacob sugiere que el «regalo» de la infraestructura de las comunicaciones comporta un coste, que no es otro que el de ser objeto de la vigilancia china que integra su diseño.

Espionaje del sector privado

[1]. *Mata tu televisión* es el nombre de una forma de protesta en contra de las comunicaciones masivas, y en la que las personas rehúyen de la televisión en sus actividades sociales.

[2]. El «efecto de red» es el efecto que tiene una persona que realiza una actividad en las probabilidades de que otra persona realice dicha actividad.

[3]. Para ampliar información sobre la investigación del gran jurado, véase la «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[4]. Según el diario *The Wall Street Journal*: «El gobierno estadounidense ha obtenido un controvertido tipo de orden judicial secreta para obligar a Google Inc. y al pequeño servidor de Internet Sonic.net, a ceder información sobre las cuentas de correo del voluntario de WikiLeaks, Jacob Appelbaum, según confirman los documentos revisados por *The Wall Street Journal* [...] El caso WikiLeaks se convirtió en un banco de pruebas en cuanto a la interpretación de la ley cuando meses antes Twitter recurrió judicialmente la orden que le instaba a ceder los registros de las cuentas de todos los simpatizantes de WikiLeaks, incluido el Sr. Appelbaum [...] La orden también requería el "protocolo de Internet" o direcciones IP de los dispositivos desde los cuales éstos accedían a sus cuentas. Una dirección IP es un número único asignado al dispositivo conectado a Internet. La orden también demandaba las direcciones de correo de aquellos con quienes dichas cuentas mantenían comunicación. El contenido de la citación se declaró secreto, sin embargo, Twitter logró que judicialmente se le otorgara el derecho de notificar a los subscriptores la información que les había sido reclamada [...] Las citaciones revisadas por el diario buscan el mismo tipo de datos que los que se solicitaron a Twitter. La citación secreta a Google es de fecha 4 de enero y se remite al gigante con la intención de obtener la dirección IP desde la que el Sr. Appelbaum accedía a su cuenta de correo gmail.com, así como las direcciones de

correo electrónico y las direcciones IP de los usuarios con quienes éste se comunicó desde el 1 de noviembre del año 2009. No está claro si Google recurrió la citación o si finalmente cedió la información. La citación secreta enviada a Sonic es de fecha 15 de abril y requiere la misma información que el resto de citaciones sobre el Sr. Appelbaum. El 31 de agosto el tribunal accedió a levantar el secreto de la orden remitida a Sonic y suministrar una copia de la misma al Sr. Appelbaum. "Secret orders target email"». *The Wall Street Journal*, 9 de octubre de 2011: http://online.wsj.com/article/SB10001424052970203476804576 (último acceso 11 de octubre de 2012). Para más detalles véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[5]. «WikiLeaks pide a Google y a Facebook que revelen el contenido de las citaciones judiciales recibidas», *The Guardian*, 8 de enero de 2011: http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas (último acceso 16 de octubre de 2012).

Véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate para más información al respecto.

[6]. Véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[7]. Para más información, véase el sitio web Europa versus Facebook: http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html (último acceso 24 de octubre de 2012).

[8]. Una Carta de Seguridad Nacional o NSL (National Security Letter), es una carta remitida por una agencia gubernamental estadounidense solicitando «información sin contenido» o «metadatos» tales como registros de transacciones económicas, direcciones IP o contactos de correo electrónico. Cualquiera que reciba este tipo de carta está obligado a remitir dichos registros, pues de lo contrario se enfrenta irremisiblemente a un proceso judicial. Las cartas de seguridad nacional no requieren de autorización judicial —pueden ser remitidas directamente por una agencia federal. Por este motivo son similares a las denominadas «citaciones administrativas», órdenes para conseguir información que sólo necesitan supervisión administrativa. Sobre esta base, se puede decir que las cartas de seguridad nacional violan de manera flagrante las protecciones que otorga la Cuarta Enmienda frente a los registros y confiscaciones arbitrarios. Las cartas de seguridad nacional también contienen un «elemento mordaza» al calificar de delito penal el que una persona que reciba este tipo de cartas hable de ello con un tercero. Sobre esta base, se puede decir que las cartas de seguridad nacional violan de manera flagrante las protecciones de la Primera Enmienda sobre la libertad de expresión. En el caso Doe versus Gonzales, la cláusula de silencio incluida en las cartas de seguridad nacional fue declarada inconstitucional. La ley se modificó para garantizar a los receptores de este tipo de

cartas el derecho a impugnarlas por la vía judicial, sin embargo, para satisfacción del Tribunal de Apelaciones del Segundo Circuito las cartas de seguridad nacional no volvieron a declararse inconstitucionales. Las cartas de seguridad nacional siguen siendo criticadas por grupos que defienden las libertades civiles, e impugnadas en los tribunales.

El uso de las cartas de seguridad nacional se ha incrementado notablemente tras la aprobación de la Ley PATRIOTA de EE.UU. en el año 2001. Los receptores de este tipo de cartas suelen ser proveedores de servicios, como ISPs o instituciones financieras. Los registros solicitados suelen estar relacionados con los clientes del receptor. El receptor no puede informar a su cliente del requerimiento de sus registros. Si bien los receptores tienen derecho a impugnar las cartas de seguridad nacional ante los tribunales, la cláusula de silencio impide que el interesado llegue a enterarse y, por ende, que éste pueda impugnar la carta ante los tribunales. Para ilustrar lo complicado que es justificar esta actuación, véase el vídeo de la viceconsejera general del FBI tratando de responder a la pregunta de Jacob Appelbaum: «¿Cómo puedo yo acudir a un tribunal si el tercero que recibe la citación no puede informarme de que estoy siendo investigado por ustedes?» Su respuesta fue: «Hay momentos en que tenemos que poner ese tipo de cosas en su sitio». Es espeluznante:

http://youtu.be/dTuxoLDnmJU (también aparece con material adicional en Privacy SOS: http://privacysos.org/node/727).

Según la Fundación de Fronteras Electrónicas: «De entre los poderes de vigilancia gubernamental más peligrosos que han proliferado con la Ley PATRIOTA de EE.UU., el poder que otorga el título 18, artículo 2709, sección 505 de la Ley PATRIOTA es uno de los más aterradores e invasivos. Estas cartas remitidas a proveedores de servicios de comunicación como compañías telefónicas y suministradoras de dominios permiten al FBI recabar información secreta relacionada con las comunicaciones y la actividad en la red de cualquier ciudadano americano sin una supervisión significativa o la revisión previa de un juez. Los receptores de las cartas de seguridad nacional están sujetos a la cláusula de silencio que, además de al público en general, les prohíbe revelar la existencia de las mismas a sus empleados, amigos, o incluso a sus familiares.» Véase: https://www.eff.org/issues/national-security-letters. Véase también la recopilación de documentos relacionados con las cartas de seguridad nacional publicada por la Fundación de Fronteras Electrónicas al amparo de la Ley de Libertad de Información: https://www.eff.orgs/issues/foia/07656JDB (último acceso a todos los enlaces incluidos en esta nota 23 de octubre de 2012).

Combatir la vigilancia total con las leyes de la física

[1]. Véase la nota 41 sobre las Primeras cripto-guerras de la década de los noventa.

[2]. Julian se refiere al SSL/TLS, un protocolo criptográfico actualmente incorporado como protocolo estándar en todos los navegadores web y utilizado para la navegación segura —un ejemplo son los navegadores utilizados en la banca online.

[3]. Por citar uno entre los muchos ejemplos que existen, véase: «Blackberry y Twitter encienden las revueltas en Londres», Bloomberg, 9 de agosto de 2011: http://www.bloomberg.com/news/2011-08-09/blackberry-messages-probed-in-u-k-rioting-as-police-say-looting-organized.html (último acceso 16 de octubre de 2012).

[4]. Por ejemplo, el miembro de LulzSec que reveló la existencia de fallos en la política de seguridad de Sony al sacar a la luz los datos personales de los clientes de Sony fue arrestado tras recabarse su identidad del sitio proxy HideMyAss.com, vía orden judicial dictada en EE.UU. Véase: «Hacker de LulzSec declarado culpable del ataque a Sony», BBC, 15 de octubre de 2012: http://www.bbc.com/news/tecnology-19949624 (último acceso 15 de octubre de 2012).

Internet y la política

[1]. SOPA, siglas en inglés que hacen referencia a la Ley de cese a la piratería en línea. PIPA, siglas en inglés que hacen referencia a la Ley de protección de la propiedad intelectual. Ambos son proyectos de ley propuestos en EE.UU. que han alcanzado especial relevancia mundial a principios del año 2012. Ambos son fiel reflejo del deseo de la industria de contenidos, representada por instituciones como la *Recording Industry Association of America*, de implantar una ley global de propiedad intelectual lo más restrictiva posible, en respuesta a la libre distribución de manifestaciones culturales en la red. Ambas leyes proponen otorgar amplios y estrictos poderes de censura a las agencias del orden estadounidenses, que amenazan con «romper internet». Ambas leyes han desatado la ira de importantes sectores de la comunidad virtual internacional, y han provocado una dura reacción por parte de actores industriales con intereses en una internet libre y abierta. A principios de 2012, Reddit, Wikipedia y varios miles de sitios web fundieron a negro sus servicios en señal de protesta, generando una gran presión sobre los representantes públicos. Otros proveedores de servicios como Google, alentaron las peticiones en contra. En respuesta, ambas leyes fueron suspendidas y continúan a la espera de reconsideración y debate sobre si realmente representan el

mejor enfoque al problema de la propiedad intelectual online. El episodio encarna la primera acción de poder efectivo de los grupos de influencia de la industria en internet.

[2]. Véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[3]. ACTA siglas que en inglés hacen referencia al Acuerdo Comercial de la Lucha contra la Falsificación. Un tratado multilateral negociado en secreto durante años y liderado por Estados Unidos y Japón. Este acuerdo establece en su mayoría nuevas y draconianas obligaciones para proteger la propiedad intelectual.

Los primeros borradores del ACTA fueron revelados al público en el año 2008, tras su filtración a WikiLeaks, generando clamorosas protestas por parte de activistas culturales y defensores de la red. Véase el apartado del ACTA en WikiLeaks: http://wikileaks.org/wiki/Category:ACTA

Los cables diplomáticos de EE.UU. remitidos a La Quadrature Du Net por WikiLeaks a principios de 2011 demuestran que el ACTA fue negociado en secreto expresamente para agilizar la creación de una rigurosa y extrema normativa de propiedad intelectual, que luego se impondría a los países más pobres originariamente excluidos del tratado. Véase: «Los cables de Wikileaks arrojan luz sobre la historia del ACTA», La Quadrature Du Net, 3 de febrero de 2011: http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history (último acceso 23 de octubre de 2012).

En julio de 2012, tras la campaña liderada por La Quadrature Du Net y Jérémie Zimmermann, el ACTA fue rechazado en el Parlamento Europeo.

[4]. M.A.I.D (Mutually) Assured Information Destruction. Es un soporte que proporciona un depósito de claves remoto de sensibilidad temporal y autentificación demostrable con una codificación opcional de socorro/emergencia. Destruye de forma automática las claves criptográficas una vez rebasado cierto umbral temporal programable: https://www.noisebridge.net/wiki/M.A.I.D. Legislación como la Ley de reglamentación de los poderes de investigación del año 2000 también conocida como RIPA por sus siglas en inglés, convierte al Reino Unido en un régimen bastante hostil para la criptografía. Según esta ley, los individuos pueden ser obligados a descifrar información o a entregar una contraseña a petición de cualquier agente de policía. No se requiere supervisión judicial. La negativa a colaborar puede derivar en una denuncia penal. En el proceso judicial subsiguiente, si el acusado manifestara que ha olvidado la contraseña, se invierte la carga de la prueba. Para evitar la condena el acusado debe probar que en efecto ha olvidado dicha clave. Esto ha sido reiteradamente cuestionado por los detractores de la ley, dado que parte de una presunción de culpabilidad. Comparativamente, si bien en Estados Unidos se han iniciado multitud de litigios relacionados con este asunto y la situación no es ni mucho menos ideal, el porcentaje de éxito ha sido mucho mayor cuando se han invocado la Primera y la Cuarta Enmiendas en situaciones

similares. Véase el informe «Libertad de Sospecha, Reforma de Vigilancia para la Era Digital» publicado por JUSTICE el 4 de noviembre de 2011, disponible en: http://www.justice.org.uk/resources.php/305/freedom-from-suspicion. Para ampliar información sobre el sistema de archivos Rubberhose, véase: «Los idiotas sabios. Guía para el programa Rubberhose», por Suelette Dreyfus: http://marutukku.org/current/src/doc/maruguide/t1.html (último acceso a todos los enlaces 24 de octubre de 2012).

[5]. Un archivo de la antigua lista de correo Criptopunk puede descargarse de: http://cryptome.org/cpunks/cpunks-92-98.zip.

Tim May fue miembro fundador de la lista de correo Criptopunk. Véase su Cyphernomicon (documento escrito por Tim), elaborado a modo de guía de preguntas y respuestas en torno a la filosofía e historia del movimiento criptopunk:
http://cypherpunks.to/faq/cyphernomicon/cyphernomicon.ht
(último acceso a ambos enlaces 24 de octubre de 2012).

[6]. «Acuerdo multilateral sobre propiedad intelectual propuesto por EE.UU. (2007)», WikiLeaks, 22 de mayo de 2008: http://wikileaks.org/wiki/Proposed_US_ACTA_multi-lateral_intellectual_property_trade_agreement_%282007%29 (último acceso 21 de octubre de 2012).

[7]. «Desmantelamiento masivo de vídeos anticienciología en You Tube» Fundación Fronteras Electrónicas, 5 de septiembre de 2008: https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube (último acceso el 16 de octubre de 2012).

[8]. «Borrador de acuerdo de libre comercio EE.UU.-India, 24 de febrero de 2009». WikiLeaks, 23 de junio de 2009: http://wikileaks.org/wiki/EU-India_Free_Trade_Agreement_draft,_24_Feb_2009 (último acceso 21 de octubre de 2012).

[9]. Peer-to-Peer o P2P hace referencia a una red en la que cada ordenador puede actuar como un cliente o como un servidor para todos los demás (cada ordenador puede tanto dar como recibir información), permitiendo el rápido intercambio de contenidos (música, vídeos, documentos o cualquier otro tipo de información digital).

[10]. *Cloud computing* o computación en la nube describe una situación en la que muchas funciones tradicionalmente realizadas por un ordenador, como el almacenamiento de datos (incluidos los datos de usuario para distintas aplicaciones), alojar y operar software, y ofrecer capacidad de procesamiento para operar el software, se efectúan remotamente, fuera del propio ordenador, «en la nube» — generalmente por empresas que ofrecen servicios de computación en la nube vía internet. En lugar de necesitar un ordenador personal completo, todo cuanto el usuario necesita es un dispositivo con acceso a internet, todo lo demás se le ofrece a través de la red. La metáfora «en la nube» esconde el hecho de que todos los datos y metadatos del usuario están realmente alojados en un ordenador remoto sito en algún centro de datos, controlado con toda probabilidad por una gran multinacional como Amazon, lo cual quiere decir que si bien los usuarios han dejado de controlar su información, un tercero lo hace por ellos.

[11]. Véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[12]. DIASPORA es una red social que permite a cada uno de sus usuarios actuar haciendo las veces de su propio servidor mediante la instalación del software DIASPORA, lo cual les permite mantener el control de su propia información. Se creó como alternativa de privacidad a Facebook. Es una red sin ánimo de lucro cuya propiedad pertenece a los usuarios: http://diasporaproject.org.

[13]. El Napster original (1999-2001) era un servicio pionero P2P para compartir música. Fue tremendamente popular hasta que fue clausurado oficialmente por vulnerar los derechos de autor a consecuencia de las acciones legales emprendidas por la *Recording Industry Association of America*. Tras la quiebra de la empresa, el nombre «Napster» se compró y se utilizó como marca de una nueva tienda de venta de música online.

[14]. Véase «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[15]. Benjamin Bayart es el presidente de French Data Network, la proveedora de servicios de internet en activo más antigua de Francia, y un acérrimo defensor de la neutralidad de la red y del software libre. Véase su entrada en Wikipedia (en francés): http://fr.wikipedia.org/wiki/Benjamin_Bayart (último acceso 15 de octubre de 2012).

[16]. Larry Lessig es un académico y activista americano mayormente conocido por sus reflexiones sobre los derechos de autor y la cultura libre. Publica sus entradas en el blog: http://lessig.tumblr.com (último acceso 15 de octubre de 2012).

Internet y la economía

[1]. Hay una enorme cantidad de contenido fascinante sobre los cables diplomáticos de EE.UU. revelados por WikiLeaks sobre este asunto. Objeto de un interesante debate son los siguientes cables (todos ellos consultados por sus respectivas referencias el 24 de octubre de 2012):

07BEIRUT1301:http://wikileaks.org/cable/2007/08/07BEIRU

08BEIRUT490:
http://wikileaks.org/cable/2008/04/08BEIRUT490.html

08BEIRUT505:
http://wikileaks.org/cable/2008/04/08BEIRUT505.html

08BEIRUT523:
http://wikileaks.org/cable/2008/04/08BEIRUT523.html

[2]. Véase el cable de referencia ID 10MOSCOW228, WikiLeaks:http://wikileaks.org/cable/2010/02/10MOSCOW228 (último acceso 24 de octubre de 2012).

[3]. Para ampliar información sobre los asesinatos arbitrarios de los ciudadanos estadounidenses Anwar al-Awalaki y su hijo Abdulrahman al Awlaki, véase la columna de Gleen Greenwald: «El asesinato arbitrario de ciudadanos estadounidenses es ahora una realidad» en el blog Salon.com del 30 de septiembre de 2011: http://www.salon.com/2011/09/30/awlaki_6. Y: «The_Killing_of_Awlaki's_16-year_old_son.»

Es literalmente imposible imaginar una repudiación más flagrante de los principios básicos de la república que el desarrollo de una agencia gubernamental de carácter secreto prácticamente omnipotente que simultáneamente recopila información sobre los ciudadanos y luego aplica una «matriz de disposiciones» para determinar qué castigo debe imponer. Esto es una distopía política clásica convertida en realidad —Glenn Greenwald: «Obama da pasos para perpetuar la guerra contra el terrorismo», *The Guardian,* 24 de octubre de 2012: http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-kill-list (o la lista de la muerte de Obama); (último acceso a estos enlaces el 24 de octubre de 2012).

[4]. Para ampliar información, podéis consultar la bibliografía de Anonimity, Documentos seleccionados en Anonimity, a cargo de Roger Dingledine y Nick Mathewson: http://freehaven.net/anonibib (último acceso 24 de octubre de 2012).

La moneda *chaumiana* se emite de manera centralizada, pero utiliza la criptografía para garantizar transacciones anónimas. La moneda *chaumiana* contrasta con el Bitcoin, otra moneda electrónica analizada exhaustivamente a continuación, donde todas las transacciones son públicas, aunque carece de autoridad central.

[5]. Para ampliar información sobre el bloqueo bancario a WikiLeaks véase la «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[6]. Julian está haciendo referencia a los planes del gobierno británico de incrementar el uso de pulseras electrónicas. Véase: «Se planea implantar la pulsera electrónica a más de cien mil delincuentes», *The Guardian*, 25 de marzo de 2012: http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice (último acceso 22 de octubre de 2012).

En el momento del debate Julian estaba bajo arresto de domiciliario, a expensas del resultado de su caso de extradición. Tras ser confinado sin cargos en una celda de aislamiento en diciembre de 2010, Julian estuvo detenido bajo arresto domiciliario tras pagar una fianza por un importe superior a las 300.000 libras. Una de las condiciones de su fianza era su confinamiento en una dirección concreta durante ciertas horas, y este régimen se aplicaba a través de una pulsera electrónica colocada en su tobillo que controlaba una empresa privada de seguridad contratada por el gobierno británico. Todos los movimientos de Julian eran controlados hasta el punto de obligarle a fichar diariamente en una comisaría de policía, a una hora determinada, durante más de 550 días. En el momento de la publicación de este libro, Julian vive confinado en la Embajada de Ecuador en Londres, rodeada a todas horas de la policía metropolitana de Londres. En junio de 2012, Julian entró en la embajada pidiendo asilo político a causa de la persecución que

padecía por parte del gobierno de Estados Unidos y sus aliados. El asilo le fue concedido en el mes de agosto de 2012.

[7]. «¿Está la CCA (Corrections Corporation of America) tratando de apoderarse del mundo?», Unión Americana de Libertades Civiles, 21 de febrero de 2012:

http://www.aclu.org/blog/prisoners-rights/cca-trying-take-over-world.

Véase también: «Goldman Sachs invertirá 9,6 millones de dólares en la rehabilitación de la cárcel de Nueva York», *The Guardian,* 2 de agosto de 2012:

http://www.guardian.co.uk/society/2012/aug/02/goldman-sachs-invest-new-york-jail (último acceso a todos los enlaces 24 de octubre de 2012).

[8]. Bitcoin (http://bitcoin.org) es la primera implantación realmente exitosa de una idea clásica del movimiento criptopunk: la moneda criptográfica digital. El Bitcoin se debate en profundidad en la obra, pero una excelente explicación introductoria sobre la tecnología y la filosofía que lo sustenta se puede encontrar en «*Understanding Bitcoin*» (Entendiendo el Bitcoin), Al Jazeera, 9 de junio de 2012:

http://aljazeera.com/indepth/opinion/2012/201253094379316 (último acceso 22 de octubre de 2012).

[9]. El oro electrónico fue una moneda digital que empezó a circular en el año 1996. Sus propietarios fueron acusados de organizar una «conspiración para blanquear dinero» por el Departamento de Justicia. Fueron declarados culpables, con penas de libertad provisional, arresto domiciliario y servicios a la comunidad. El tribunal competente declaró que las condenas habían sido indulgentes debido a que su intención primigenia no era la de participar en una actividad ilegal. Véase «*Bullion and Bandits. The improbable Rise and Fall of E-Gold*» (Lingotes y bandidos. El improbable ascenso y desplome del oro electrónico), *Wired*, 9 de junio de 2009: http://www.wired.com/threatlevel/2009/06/e-gold (último acceso 22 de octubre de 2012).

[10]. Antes del nacimiento de internet, la red X.25 era la mayor red global de intercambio de datos que coexistía con la red telefónica. La facturación sobre la X.25 se basaba en la cantidad de datos enviados y recibidos, y no en la longitud/distancia de una conexión, como ocurre con la red telefónica. Las pasarelas (o PADs) permitían al usuario conectarse a la red X.25 desde una red telefónica a través de módems o acopladores acústicos. Más información en Wikipedia:

http://en.wikipedia.org/wiki/X.25 (último acceso 24 de octubre de 2012).

[11]. David Chaum es criptógrafo e inventor de protocolos criptográficos. Es un pionero en tecnologías de moneda digital, y quien introdujo el *eCash* o efectivo electrónico, una de las primeras monedas electrónicas criptográficas y anónimas.

[12]. Sobre el efecto de los comentarios negativos de la prensa, véase: «El Bitcoin implosiona, cae más del 90 por ciento desde el pico de junio», *Arstechnica*, 18 de octubre de 2011: http://artstechnica.com/tech-policy/2011/10/bitcoin-implodes-down-more-than-90-percent-from-june-peak (último acceso 22 de octubre de 2012).

[13]. Véase por ejemplo: «La página web clandestina donde puedes comprar cualquier droga imaginable», Gawker, 1 de junio de 2011: http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable (último acceso 22 de octubre de 2012).

[14]. El trabajo original de Lawrence Lessig sobre los derechos de autor y la cultura (reflejado por ejemplo en la obra titulada *Free Culture* (2004), ha sido reemplazado en los últimos años por el interés de corromper la democracia americana a través de las continuas presiones de los lobbies en el congreso. Véase: The Lessig Wiki: http://wiki.lessig.org.

[15]. La unión californiana de guardias penitenciarios (California Correctional Peace Officers Association) es un grupo de poder de especial relevancia en California que por lo general dona sumas de siete cifras en las elecciones estatales, siendo, año tras año, uno de los donantes individuales más relevantes de la campaña. Véase «*The California reelin*», *The Economist*, 17 de Marzo de 2011: http://www.economist.com/node/18359882. Y «Los barrotes del estado dorado», *Reason*, julio de 2011: http://reason.com/archives/2011/06/23/the-golden-states-iron-bars. Véase también la entrada de la Asociación de guardias penitenciarios de California en la página web FollowTheMoney del National Institute for Money in State Politics: http://www.followthemoney.org/database/topcontributor.phtr u=3286&y=0 (último acceso 22 de octubre de 2012).

[16]. Heinz von Foerster (1911-2002) fue un científico austriaco-americano y un arquitecto de la cibernética. Su llamado «imperativo ético» o lema común es: «Actúa siempre de tal modo que se incrementen las alternativas», o en alemán: «Handle stets so, daβ di Anzahl der Wahlmöglichkeiten gröβer wird».

[17]. Jacob atribuye su observación a John Gilmore.

Censura

[1]. Para obtener más información sobre el acoso de Jacob y otras personas vinculadas a WikiLeaks, véase la «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[2]. Isaac Mao es un bloguero chino, arquitecto de software e inversor de capital riesgo. También es cofundador de CNBlog.org y miembro del consejo del Proyecto Tor.

[3]. Véase la página de WikiLeaks sobre Nadhmi Auchi: http://wikileaks.org/wiki/Nadhmi_Auchi (último acceso 24 de octubre de 2012).

[4]. Los artículos están disponibles en la siguiente dirección de WikiLeaks:

http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_censored_from_the_Guardian,_Observer,_Telegraph_and_N (último acceso 24 de octubre de 2012).

[5]. Como nota general tanto el sitio http://cables.mrkva.eu/ como el sitio http://cablegatesearch.net ofrecen excelentes modos de comparar las versiones editadas de los cables con las versiones completas, a fin de ver lo que los socios de comunicación de WikiLeaks han ocultado.

[6]. «El hijo de Qaddafi es bisexual y otras cosas que *The New York Times* no quiere que usted sepa», Gawker, 16 de septiembre de 2011: http://gawker.com/580809/qaddafis-son-is-bisexual-and-other-things-the-new-york-times-doesnt-want-you-to-know-about.

El ejemplo citado se refiere al cable con la referencia ID 06TRIPOLI198, WikiLeaks:

https://wikileaks.org/cable/2006/05/06TRIPOLI198.html.

Los párrafos censurados pueden observarse visualmente en el sitio web Cablegatesearch, donde se ofrece el historial de cambios, con los párrafos censurados sombreados en rosa: http://www.ablegatesearch.net/cable.php?id=06TRIPOLI198&version=1291757400 (último acceso a todos los enlaces 22 de octubre de 2012).

[7]. Para acceder al cable original véase el cable de referencia ID 10STATE17 263,WikiLeaks: http://wikileaks.org/cable/2010/02/10STATE17263.html.

Para acceder al artículo de *The New York Times* véase: «Irán refuerza su arsenal con ayuda de Corea del norte», *The New York Times,* 29 de noviembre de 2010: http://www.nytimes.com/2010/11/29/world/middleeast/29miss_r=0.

El mismo cable fue también utilizado por David Leigh de *The Guardian* para su artículo: «Los cables de WikiLeaks desvelan temores frente al programa nuclear de Pakistán», *The Guardian*, 30 de noviembre de 2010: http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-pakistan-nuclear-fears. La versión censurada del cable publicado por *The Guardian*, sin citar el número de referencia del cable, lo redujo a sólo dos párrafos relacionados con Pakistán. «Cables de la embajada de EE.UU.:XXXXXXXXXXXX», *The Guardian,* 30 de noviembre de 2010: http://www.guardian.co.uk./world/us-embassy-cables-documents/250573.

El nivel de censura puede observarse visualmente en el sitio web Cablegatesearch, que muestra el historial de cambios, con la censura de prácticamente todo el documento sombreada en rosa:

http://www.cablegatesearch.net/cable.php?id=10STATE17263&version=1291486260 (último acceso a

todos los enlaces 22 de octubre de 2012).

[8]. Para acceder al cable original véase el cable de referencia ID 08KYIV2414, WikiLeaks: http://wikileaks.org/cable/2008/12/08KYIV2414.html.

Para acceder a la versión censurada de *The Guardian* véase «Cables de la embajada de EE.UU.: el suministro de gas vinculado a la mafia rusa», 1 de diciembre de 2010: http://www.guardian.co.uk/world/us-embassy-cables-documents/182121? INTCMP=SRCH.

El nivel de censura puede observarse visualmente en el sitio web Cablegatesearch, que muestra el historial de cambios, con los párrafos censurados sombreados en rosa: http://www.cablegatesearch.net/cable.php?id=08KYIV2414&versi-on=1291255260 (último acceso a todos los enlaces 22 de octubre de 2012).

[9]. Para acceder al cable original véase el cable de referencia ID 10ASTANA72, WikiLeaks: http://wikileaks.org/cable/2010/01/10ASTANA72.html.

Para acceder a la versión censurada de *The Guardian*, véase: «Cables de la embajada de EEUU: Kazakhstan-Los cuatro grandes», *The Guardian*, 29 de noviembre de 2010: http://www.guardian.co.uk/world/us-embassy-cables-documents/24516? INTCMP=SRCH.

El nivel de censura puede observarse visualmente en el sitio web Cablegatesearch, que muestra el historial de cambios, con los párrafos censurados sombreados en rosa: http://www.cablegatesearch.net/cable.php?id=10ASTANA72&version=1291113360 (último acceso a todos los enlaces 22 de octubre de 2012).

[10]. Véase por ejemplo el cable de referencia ID 09TRIPOLI413 sobre las compañías energéticas occidentales que operan en Libia. La representación visual que muestra el sito web Cablegatesearch, con los párrafos censurados sombreados en rosa reflejan que *The Guardian* eliminó toda referencia a los nombres de las compañías energéticas y sus directivos, a excepción de las referencias que aludían a la compañía de energía rusa Gazprom. No obstante parte del contenido es, en cierto sentido, atenuante para las compañías occidentales, las modificaciones son notables, y la versión censurada ofrece una foto bastante diferente:

http://www.cablegatesearch.net/cable.php?id=09TRIPOLI413&version=1296509820 (último acceso 22 de octubre de 2012).

[11]. En este ejemplo el cable original contenía 5.226 palabras. La versión censurada publicada por *The Guardian* sólo tenía1.406 palabras.

Para acceder al cable original véase el cable de referencia ID 05SOFIA1207, WikiLeaks: http://wikileaks.or/cable/2005/07/05SOFIA1207.html.

Para acceder a la versión censurada de *The Guardian*, véase: «Cables de la embajada de EEUU: Crimen organizado en Bulgaria», 1 de diciembre de 2010: http://www.guardian.co.uk/world/us-embassy-cables-documents/36013.

Para acceder al artículo de *The Guardian* basado en el cable véase: «Los cables de WikiLeaks: el gobierno ruso utiliza a la mafia para el trabajo sucio», *The Guardian*, 1 de diciembre de 2010: http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia.

El nivel de censura puede observarse visualmente en el sitio web Cablegatesearch, que refleja el historial de cambios con los párrafos censurados sombreados en rosa: http://www.cablegatesearch.net/cable/php?id=05SOFIA1207&version=1291757400.

El ejemplo búlgaro se debate por el socio de comunicación búlgaro de WikiLeaks, Bibol en «Cable inédito desde Sofía refleja la absoluta invasión del estado por parte del crimen organizado (última hora: Comparación del cable)», WL

Central, 18 de marzo de 2011: http://wlcentral.org/node/1480. Además véase: «*The Guardian*: ¿Ocultando, censurando o mintiendo?» WL Central, 19 de marzo de 2012: http://wlcentral.org/node/1490. Véanse también, debajo de ambos artículos, los comentarios del periodista David Leigh y las respuestas que suscitan (último acceso a todos los enlaces 22 de octubre de 2012).

[12]. Esto alude al cable de referencia ID 09BERLIN1108. El nivel de censura puede observarse visualmente en el sitio web de Cablegatesearch, que muestra el historial de cambios con los párrafos censurados sombreados en rosa: http://www.cablegatesearch.net/cable.php?id=09BERLIN1108&version=1291380660 (último acceso 22 de octubre de 2012).

[13]. Más ejemplos en el sitio web the cabledrum: www.cabledrum.net/pages/censorship.php.

[14]. «Interceptación de telecomunicaciones. La Presidencia aportó información sobre el estado de las cosas...Recordó la mala prensa que este asunto había tenido en los medios...En este contexto, la Presidencia reconoció que, por consiguiente, el progreso en este asunto es muy lento...Varias delegaciones expresaron sus reservas sobre la preparación de un comunicado de prensa, advirtiendo que esto podía provocar una reacción en cadena y más reacciones negativas por parte de los medios. La Comisión, aunque advirtió que su posición no había cambiado, informó a las delegaciones de que una posible vía para salir del punto muerto podría consistir en seguir una estrategia similar a la que se había seguido para hacer frente al problema de la pornografía infantil en Internet. Aun reconociendo que este es un tema diferente, también tiene una dimensión de interceptación» —Comisión Europea, reunión del grupo de trabajo de cooperación policial sobre la interceptación de las telecomunicaciones, 13 y 14 de octubre de 1999. Documento completo en: http://www.quintessenz.at/doqs/000100002292/1999_10_13.Police%20Cooperation%20Working%20Group%20mixed%20 (ultimo acceso 24 de octubre de 2012).

[15]. Véase la «Nota sobre los diversos intentos de acoso sufridos por la organización WikiLeaks y las personas asociadas con ella» que precede a este debate.

[16]. Jacob se refiere al caso Gilmore v. Gonzales, 435 F. 3d 1125 (Noveno Circuito. 2006). John Gilmore, miembro fundador del movimiento criptopunk, llevó el caso hasta la Corte Suprema de EE.UU. con el fin de desvelar el contenido de una ley secreta —una Directiva de Seguridad—, que limitaba el derecho de los ciudadanos de viajar en avión sin identificación. Además de cuestionar la constitucionalidad de tal disposición, Gilmore estaba cuestionando el hecho de que la disposición en sí misma fuera secreta y que no pudiera revelarse, aun teniendo carácter vinculante para los ciudadanos estadounidenses. El tribunal revisó la Directiva de Seguridad a puerta cerrada y falló en contra de Gilmore en el punto relativo a la constitucionalidad de la Directiva. No obstante, el contenido de dicha ley nunca llegó a desvelarse en el transcurso del litigio. Véase Gilmore v Gonzales en PapersPlese.org: http://papersplease.org/gilmore/facts.html (último acceso 22 de octubre de 2012).

[17]. Christiania es un área autoproclamada independiente en Copenhague, Dinamarca. Un antiguo cuartel militar fue ocupado en la década de 1970 por una comunidad con marcado carácter colectivista y anarquista, que ha forjado un estatus legal único en Dinamarca.

[18]. El principio de la «neutralidad de la red» defiende que se prohíba (por lo general a través de la ley) que los Proveedores de Servicios de Internet (ISPs) limiten los derechos de acceso de los usuarios a las redes que conforman Internet, y también a los contenidos. Véase la página de la Fundación de Fronteras Electrónicas sobre la neutralidad de la red: https://www.eff.org/issues/net-neutrality (último acceso 22 de octubre de 2012).

[19]. «El bloqueo de los emails de WikiLeaks obstaculiza el proceso de Bradley Manning», *Politico*, 15 de Marzo de 2012: http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-117573.html (último acceso 21 de octubre de 2012).

[20]. Para ampliar información sobre Wau Holland véase la fundación de Wau Holland; http://www.wauland.de.

Privacidad para el débil, transparencia para el poderoso

[1]. «La Stasi sigue a cargo de los archivos de la Stasi», WikiLeaks, 4 de octubre de 2007: http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi (último acceso 22 de octubre de 2012).

Ratas en la ópera

[1]. «Eh aquí lo que puedes hacer para cambiar el mundo, en este preciso instante, para bien. Coge todo el dinero que se gasta en armamento y defensa cada año, y e inviértelo en alimentar, vestir y educar a los pobres del mundo sin excluir a un sólo ser humano. Y también podríamos explorar el espacio, juntos, tanto el interior y el exterior, para siempre, en paz» —Bill Hicks. Véase vídeo: «Bill Hicks-Positive Drugs Story»: http://yutu.be/vX1CvW38cHA (último acceso 24 de octubre de 2012).

[2]. La Ley Sabarnes-Oxley de 2002, es una ley estadounidense aprobada en respuesta a los escándalos corporativos y contables de Enron, Tyco International, Adelphia, Peregrine Systems y WorldCom. La ley aspiraba a erradicar el tipo de prácticas corruptas que habían llevado a todas ellas a la quiebra. La sección 1107 de la ley, artículo 1513 (e) del Código de EE.UU., establece como delito cualquier tipo de represalia ejercitada contra posibles denunciantes.

[3]. Evgeny Morozov, La desilusión de la red: El lado oscuro de la libertad de Internet (Public Affairs, 2011).

[4]. En relación con el software libre, véase «La definición de software libre» en el sitio web de GNU Operating System: http://www.gnu.org/philosophy/free-sw.html.

Hardware libre es un hardware que no está gravado con patentes de propiedad, de dominio público, donde no existen leyes que regulen la ingeniería inversa, la alteración o la falsificación (es decir leyes anti-elusión), donde los principios de diseño, las instrucciones y planes están disponibles gratuitamente para que cualquiera que disponga de ellos y de los recursos necesarios pueda construir una réplica.

Para ampliar información sobre el hardware libre véase: *Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DID;* EHSM: http://ehsm.eu. Véase también «Hardware libre» en Wikipedia: https://es.wikipedia.org/wiki/Hardware_Libre (último acceso a todos los enlaces 24 de octubre de 2012).

[5]. Sobre la impresión en 3D utilizando hardware libre y abierto véase el vídeo introductorio de la impresora en 3D RedRap: http://vimeo.com/5202148 (último acceso 24 de octubre de 2012).

[6]. «*Be the trouble you want to be in the world*» cita extraída de A Softer World, un *webcomic* fotográfico: http://www.asofterworld.com/index.php.'id=189 (último acceso 24 de octubre de 2012).

[7]. Para seguir cualquiera de los temas tratados en este debate, Jacob recomienda las siguientes fuentes bibliográficas:

La bibliografía de Anonimity, documentos seleccionados en Anonimity, a cargo de Roger Dingledine y Nick Mathewson:

http://freehaven.net/anonbib

La bibliografía de la censura, documentos seleccionados sobre censura, a cargo de Philipp Winter:

www.cs.kau.se/philwint/censorbib (último acceso a ambos enlaces 24 de octubre de 2012).

[8]. Nota al pie dejada intencionadamente en blanco.

[9]. Newaat.org es un blog colectivo independiente de Túnez creado en el año 2004: http://nawaat.org/portail. Tunileaks fue lanzada por Newaat en noviembre de 2010, publicando los cables de WikiLeaks relacionados con Túnez: https://tunileaks.appspot.com.

Para ampliar información sobre Tunilinks y la censura del gobierno de Ben-Ali, véase: «Túnez, la censura continua mientras los cables de WikiLeaks siguen circulando» Global Voices Advocacy, 7 de diciembre de 2010: http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds (último acceso a todos los enlaces 24 de octubre de 2012).

Cypherpunks
Julian Assange

Título original: *Cypherpunks*

Deusto es un sello editorial de Centro Libros PAPF, S. L. U.
Grupo Planeta, Av. Diagonal, 662-664, 08034 Barcelona (España)
www.planetadelibros.com

Primera edición en libro electrónico (epub): abril de 2013

ISBN: 978-84-234-1639-4 (epub)

Conversión a libro electrónico: Víctor Igual, S. L.
www.victorigual.com